Proceedings of the Indian Academy

(Mathematical Sciences)

Volume 97, 1987

CONTENTS

Foreword . . . . . .

The characters of supercuspidal representations as wei
integrals . . . . . .

On the proof of the reciprocity law for arithmetic Siegel moc
. . . . . *Wa*

On some generalizations of Ramanujan's continued fraction ide
. . . . . *S Bhargava, Chandrashekar Adiga and D I*

On the set of discrete subgroups of bounded covolume in a sen
. . . . . .

Explicit Ramanujan-type approximations to pi of high order. .
. . . . . *J M Borwein an*

Approximation of exponential sums by shorter ones. . . .

On endomorphisms of degree two. . . . . .

Traces of Eichler-Brandt matrices and type numbers of qu
. . . . . .

The Hecke-algebras related to the unimodular and modu
Hurwitz order of integral quaternions . . . . . .

Poincaré series for $SO(n, 1)$. . . *Jian-Shu Li, I Piatetski-Sh*

Fluctuations in the mean of Euler's phi function . . . . . *H*

On the supersingular reduction of elliptic curves . . . . . .

The Manin–Drinfeld theorem and Ramanujan sums. . . .
. . . . . *V Kumar Murty and Din*

On Ramanujan's modular identities. . . . . .

Hypergeometric series and continued fractions . . . . . .

Multiplicative properties of the partition function . . . . .
. . . . . *A Sch*

The states of the character ring of a compact group . . . .

On an approximate identity of Ramanujan . . . . . .

Subject index . . . . . .

Author index . . . . . .

Dedicated to the memory of

SRINIVASA RAMANUJAN

on the occasion of the birth centenary

Foreword

The life and work of Srinivasa Ramanujan are of unique significar of mathematics, professionals and amateurs alike. It is a matte India, that despite the unfortunate brevity of his life and lack of work continues, even after seven odd decades, to generate new an and more and more of it is being applied outside mathematic towering genius is, on the other hand, an invaluable reminder t confidence our potentialities as also to keep up a dynamic interac mainstream.

As our tribute on the occasion of the Birth Centenary we are this Special Issue of the Proceedings (Mathematical Sciences) of t of Sciences dedicated to Srinivasa Ramanujan. We have attempt readers papers of eminent mathematicians in a broad spectrum of a centring around, but not limited to, Ramanujan's interests. We a to our contributors for their crucial role in making this volume

December 1987

Chairn
Proceedings (Ma

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 3–
© Printed in India.

The characters of supercuspidal representations as weighted orbital integrals

JAMES ARTHUR*
Department of Mathematics, University of Toronto, Toronto,

Abstract. Weighted orbital integrals are the terms which occur trace formula. We shall investigate these distributions on a p-a the weighted orbital integral of a supercuspidal matrix coef corresponding character.

Keywords. Supercuspidal representation; weighted orbital inte

1. Introduction

Let G be a reductive algebraic group over a non-Archime characteristic 0. Suppose that π is a (smooth) supercuspidal re a complex vector space V. Let $f(x)$ be a finite sum of matrix

$$\xi(\pi(x)^{-1}v), \quad x\in G(F), \quad v\in V, \quad \xi\in V^*.$$

Then f is a locally constant function on $G(F)$ which is compa the split component A_G of the centre of G. If Θ_π is the chara

$$\Theta_\pi(f) = \int_{A_G(F)\backslash G(F)} f(x)\Theta_\pi(x)\mathrm{d}x.$$

We are going to study the weighted orbital integrals of f.

Suppose that M is a Levi component of some parabolic s defined over F. The set $\mathcal{P}(M)$ of all parabolic subgroups over

equals

$$(-1)^{\dim(A_M/A_G)}\Theta_\pi(f)\Theta_\pi(\gamma).$$

Observe that the second expression depends on a cho
$A_G(F)\backslash G(F)$; the first expression depends on choices of i
and $A_M(F)\backslash G(F)$. There is a compatibility requirement b
on $A_M(F)/A_G(F)$ and the measure on $\mathbf{a}_M/\mathbf{a}_G$.

The theorem is a p-adic version of a similar result for rea
It tells us that the character values of π on a non-comp
as the weighted orbital integrals of a matrix coefficient of
that the result is part of a larger theory. Kazhdan has
proving a local trace formula for G. The idea would be
of the left-right convolution operator of a pair of funct
spectrum of $L^2(G(F))$. Our theorem could be regarded as
of the two functions is the matrix coefficient f. A differer
undiscovered) trace formula is provided by work of W
return to the question on another occasion.

For $G = SL(2)$, the theorem was first established by K
indebted to him for enlightening conversations.

2. Positive orthogonal sets

Let us recall the precise definition of $v_M(x)$. It depends on
subgroup K of $G(F)$ which is in good position relative
vertex of K in the building of G lies in the apartment of
For any parabolic subgroup $P\in\mathscr{P}(M)$, with Levi decom
point $x\in G(F)$, we can write

$$x = n_P(x)m_P(x)k_P(x),$$

with $n_P(x)\in N_P(F)$, $m_P(x)\in M(F)$ and $k_P(x)\in K$. Set

$$H_P(x) = H_M(m_P(x)),$$

The function $v_M(x)$ equals the volume of the convex hull of t

$$\{-H_P(x): P \in \mathscr{P}(M)\}$$

onto $\mathbf{a}_M/\mathbf{a}_G \cong \mathbf{a}_M^G$.

It is convenient to choose a suitable Euclidean metric $\|\cdot\|$ to normalize the Haar measures on $\mathbf{a}_M$, $\mathbf{a}_G$ and $\mathbf{a}_M/\mathbf{a}_G$. These m Haar measures on $A_M(F)$, $A_G(F)$ and $A_M(F)/A_G(F)$. Indeed,

$$\kappa_M = A_M(F) \cap K$$

is the maximal (open) compact subgroup of $A_M(F)$, and H_M ma onto a lattice in $\mathbf{a}_M$. We take the Haar measure on $A_M(F)$ su

$$\mathrm{vol}(\kappa_M) = \mathrm{vol}(\mathbf{a}_M/H_M(A_M(F))).$$

The cases of $A_G(F)$ and $A_M(F)/A_G(F)$ are similar, and we hav

$$\mathrm{vol}(\kappa_M/\kappa_G) = \mathrm{vol}(\mathbf{a}_M/H_M(A_M(F)) + \mathbf{a}_G).$$

The points $\{-H_P(x)\}$ form a positive orthogonal set. In ge

$$\mathscr{Y} = \{Y_P: P \in \mathscr{P}(M)\}$$

of points in $\mathbf{a}_M$ is a positive orthogonal set for M if it has For any pair P and P' of adjacent groups in $\mathscr{P}(M)$, whose ch wall determined by a simple root α in $\Delta_P \cap (-\Delta_{P'})$ of (P, A_M)

$$Y_P - Y_{P'} = r\alpha^\vee,$$

for a non-negative number r. As usual, Δ_P is the set of simp $\alpha^\vee \in \mathbf{a}_M$ is the "co-root" associated to α. Suppose that $\mathscr{Y}$ has volume in $\mathbf{a}_M/\mathbf{a}_G$ of the convex hull of $\{Y_P\}$ can be expressed

$$\lim_{\lambda \to 0} \sum_{P \in \mathscr{P}(M)} \exp[\lambda(Y_P)]\theta_P(\lambda)^{-1},$$

Then

$$\{Y_{P\cap M_Q} = Y_P : P\in\mathcal{P}(M),\ P\subset Q\}$$

is a positive orthogonal set for M, but relative to M the direct sum of the spaces $\mathbf{a}_M^{M_Q} = \mathbf{a}_M^Q$ and $\mathbf{a}_{M_Q} = \mathbf{a}_Q$ convex hull of (4) in $\mathbf{a}_M$, taken modulo $\mathbf{a}_Q$, and we characteristic function of $S_M^Q(\mathcal{Y})$. The vectors (4) all pr $\mathbf{a}_Q$. Moreover, if we fix the Levi component $L = M_Q$

$$\mathcal{Y}_L = \{Y_Q : Q\in\mathcal{P}(L)\}$$

is a positive orthogonal set for L. For simplicity, we $\sigma_L^G(\cdot,\mathcal{Y}_L)$ by $S_L(\mathcal{Y})$ and $\sigma_L(\cdot,\mathcal{Y})$ respectively.

The following geometric property is a restatement

Lemma 1: *There is a positive constant δ_M with the positive orthogonal set for M and $L\supset M$ is as above,*

$$H_M = H_M^L \oplus H_L,\quad H_M^L\in\mathbf{a}_M^L,\quad H_L\in\mathbf{a}_L,$$

is a point in $\mathbf{a}_M$ such that

$$\|H_M^L\| \leqslant \delta_M d(\mathcal{Y}),$$

then H_M belongs to $S_M(\mathcal{Y})$ if and only if H_L belongs t

Another example of a positive orthogonal set is p point. Let $M_0\subset M$ be a fixed Levi component of so over F, and let W_0 be the Weyl group of (G, A_{M_0}). to be the restriction of a Euclidean metric $\|\cdot\|$ on $\mathbf{a}_M$ Choose an element $P_0'\in\mathcal{P}(M_0)$, and let $T_{P_0'}$ be a point associated to P_0'. The Weyl group W_0 acts simply t

$$\mathcal{T} = \{T_{P_0} = sT_{P_0'} : P_0 = sP_0',\ s\in W_0\}$$

$x \in G(F)$, set

$$\mathscr{Y}(x, \mathscr{T}) = \{Y_P(x, \mathscr{T}) = T_P - H_{\bar{P}}(x) \colon P \in \mathscr{P}(M)\},$$

where $\bar{P}$ denotes the parabolic subgroup opposite to P. Beca
positive orthogonal sets, rather than a sum, $\mathscr{Y}(x, \mathscr{T})$ need not b
set. However, if $d(\mathscr{T})$ is large with respect to x, the positivity
$\mathscr{Y}(x, \mathscr{T})$ becomes a positive orthogonal set. We shall assume

3. The main geometric lemma

We shall now begin the proof of the theorem. Suppose that $\mathscr{T}$
$u(x, \mathscr{T})$ denote the characteristic function in $A_G(F)\backslash G(F)$ of th

$$x = k_1 h k_2, \quad k_1, k_2 \in K, \quad h \in A_G(F)\backslash A_{M_0}(F),$$

such that the projection onto $\mathbf{a}_{M_0}^G$ of $H_{M_0}(h)$ lies in the conve
corresponds to a special vertex,

$$G(F) = K A_{M_0}(F) K.$$

We can consequently force $u(x, \mathscr{T})$ to be identically equal to 1
subset of $A_G(F)\backslash G(F)$ simply by choosing $\mathscr{T}$ so that $d(\mathscr{T})$ is s

Our starting point for the study of the matrix coefficient f i
of results of Harish-Chandra.

Lemma 2: *Suppose that f and γ are as in the theorem. Then*

$$\Theta_\pi(f)\Theta_\pi(\gamma) = \int_{A_G(F)\backslash G(F)} f(x^{-1}\gamma x) u(x, \mathscr{T}) \mathrm{d}x,$$

whenever $d(\mathscr{T})$ is sufficiently large.

Proof: If g is any function in $C_c^\infty(G(F))$, Theorem 9 of [5] tel

supported on a compact subset of $A_G(F)\backslash G(F)$ whic
approach the Dirac measure at γ. The left hand si

$$\Theta_\pi(f)\Theta_\pi(\gamma),$$

while the right hand side converges to

$$\mathrm{vol}(K)^{-1}\int_{A_G(F)\backslash G(F)}\left(\int_K f(x^{-1}k^{-1}\gamma kx)\mathrm{d}k\right.$$

This last integrand in x is compactly supported. $u(x,\mathscr{T})$ without changing its value, as long as $d(\mathscr{T})$ becomes

$$\mathrm{vol}(K)^{-1}\int_{A_G(F)\backslash G(F)}\left(\int_K f(x^{-1}k^{-1}\gamma kx)\mathrm{d}k\right.$$

$$=\mathrm{vol}(K)^{-1}\int_{A_G(F)\backslash G(F)}\int_K f(x^{-1}k^{-1}\gamma kx)$$

$$=\int_{A_G(F)\backslash G(F)} f(x^{-1}\gamma x)u(x,\mathscr{T})\mathrm{d}x,$$

since $u(x,\mathscr{T})$ is bi-invariant under K. This establis

In view of the lemma, we may write

$$\Theta_\pi(f)\Theta_\pi(\gamma)=\int_{A_G(F)\backslash G(F)} f(x^{-1}\gamma x)u(x,\mathscr{T})$$

$$=\int_{A_M(F)\backslash G(F)} f(x^{-1}\gamma x)\left(\int_{A_M(F}\right.$$

By assumption, the centralizer of γ in $G(F)$ is comp
last integral over x may be taken over a compact se
in $G(F)$.

Proof: If Q is a group in $\mathscr{F}(M)$, we write τ_Q for the character

$$\{H \in \mathbf{a}_{M_0} : \alpha(H) > 0,\ \alpha \in \Delta_Q\}.$$

It is known that

$$\sum_{Q \in \mathscr{F}(M)} \sigma_M^Q(H, \mathscr{T})\, \tau_Q(H - T_Q) = 1,$$

for $\mathscr{T}$ as in (5), and any $H \in \mathbf{a}_M$. This is a general property of p
which is easily deduced, for example, from Langlands' comb
Lemma 2.3), ([2], Lemma 6.3). We shall actually apply the r
and $\mathscr{T}$ replaced by the set

$$\varepsilon\mathscr{T} = \{\varepsilon T_{P_0} : P_0 \in \mathscr{P}(M_0)\},$$

for a certain $\varepsilon > 0$. Having been given δ, we choose ε so that
the numbers δ_M and δ_{M_0} provided by Lemma 1.

Fix the elements $a \in A_M(F)$ and $x \in \Gamma$. The left hand side of (9) is
functions, so there is a unique group $Q \in \mathscr{F}(M)$ such that

$$\sigma_M^Q(H_M(a), \varepsilon\mathscr{T})\tau_Q(H_M(a) - \varepsilon T_Q) = 1.$$

Once Q is determined, we can write

$$\begin{aligned} ax &= am_{\bar{Q}}(x)n_{\bar{Q}}(x)k_{\bar{Q}}(x) \\ &= ad(am_{\bar{Q}}(x))n_{\bar{Q}}(x) \cdot am_{\bar{Q}}(x)k_{\bar{Q}}(x). \end{aligned}$$

Consider a root α of (Q, A_Q). Since $H_M(a)$ is the sum of a vec
chamber of Q, with a convex linear combination of points

$$\{\varepsilon T_P : P \in \mathscr{P}(M),\ P \subset Q\},$$

we have

$$\alpha(H_M(a)) \geq \varepsilon \inf_{\qquad} \alpha(T_\cdot) \geq \varepsilon d(\mathscr{T})$$

Then ax belongs to KhK. Observe also that

$$H_Q(h) = H_Q(a) + H_Q(m_{\bar{Q}}(x)),$$

so that

$$H_Q(h) = H_Q(a) + H_{\bar{Q}}(x).$$

We write

$$H_M(a) = H_M^Q(a) + H_Q(a), \quad H_M^Q(a) \in \mathbf{a}_M^Q,$$

for the decomposition of $H_M(a)$ relative to the direct

$$H_{M_0}(h) = H_{M_0}^Q(h) + H_Q(h), \quad H_{M_0}^Q(h) \in \mathbf{a}_{M_0}^Q.$$

Then there is a constant $c(\Gamma)$ such that

$$\| H_{M_0}^Q(h) \| \leqslant \| H_M^Q(a) \| + c(\Gamma),$$

for any $x \in \Gamma$ and $a \in A_M(F)$, and for h defined by (1C standard properties of height functions on $G(F)$. Nov

$$\sigma_M^Q(H_M^Q(a), \varepsilon \mathscr{T}) = 1,$$

so that $H_M^Q(a)$ belongs to the convex set $S_M^Q(\varepsilon \mathscr{T})$. It fo by the norm of the projection of any of the vectors

$$\{\varepsilon T_P : P \in \mathscr{P}(M), P \subset Q\}$$

onto $\mathbf{a}_M^Q$. Therefore,

$$\| H_M^Q(a) \| \leqslant \varepsilon \| T_P \| \leqslant \varepsilon \| \mathscr{T} \|.$$

Choose $c(\Gamma, \delta)$ to be so large that $\varepsilon \delta^{-1} c(\Gamma, \delta)$ is greate Then

simply by taking $c(\Gamma, \delta)$ large enough. Now $H_Q(a)$ is related to $H_Q(h$ Since $H_{\bar{Q}}(x)$ remains bounded, we can assume that $H_Q(h)$ also lies in to ([1] Lemma 3.2), the intersection of $\mathbf{a}_Q^+$ with $S_{M_Q}(\mathscr{T})$ is the set

$$\{H \in \mathbf{a}_Q^+ : \varpi(H - T_Q) < 0, \varpi \in \hat{\Delta}_Q\},$$

where $\hat{\Delta}_Q$ is the dual basis of $\Delta_Q^\vee$. Thus, $u(ax, \mathscr{T})$ equals 1 if and o numbers

$$\varpi(H_Q(h) - T_Q) = \varpi(H_Q(a) - Y_Q(x, \mathscr{T})), \quad \varpi \in \hat{\Delta}_Q,$$

is negative. We have now only to retrace our steps. Since $H_Q(a)$ li condition is equivalent to the assertion that $H_Q(a)$ lies in $S_{M_Q}(\mathscr{Y}(x, \mathscr{T})$ is large relative to x, so we can assume that

$$d(\mathscr{Y}(x, \mathscr{T})) \geqslant \tfrac{1}{2} d(\mathscr{T}).$$

It follows from (12) that

$$\begin{aligned} \| H_M^Q(a) \| &\leqslant \varepsilon \| \mathscr{T} \| \\ &\leqslant \varepsilon \delta^{-1} d(\mathscr{T}) \\ &\leqslant 2\varepsilon \delta^{-1} d(\mathscr{Y}(x, \mathscr{T})) \\ &\leqslant \delta_M d(\mathscr{Y}(x, \mathscr{T})), \end{aligned}$$

whenever $\mathscr{T}$ satisfies (8). Applying Lemma 1 again, we conclude th to $S_{M_Q}(\mathscr{Y}(x, \mathscr{T}))$ if and only if $H_M(a)$ belongs to $S_M(\mathscr{Y}(x, \mathscr{T}))$. This is original condition that $u(ax, \mathscr{T})$ equals 1, so the proof of the lemma

As an identity of characteristic functions, the lemma asserts that

$$u(ax, \mathscr{T}) = \sigma_M(H_M(a), \mathscr{Y}(x, \mathscr{T})), \quad \alpha \in A_M(F)/A_G(F),$$

for x and $\mathscr{T}$ as stated. It follows that $\Theta_\pi(f)\Theta_\pi(\gamma)$ equals

is any subgroup of finite index in $A_M(F)$, which co
2 and 3 as above, we obtain

$$\Theta_\pi(f)\Theta_\pi(\gamma)=\int_{A'_M\backslash G(F)} f(x^{-1}\gamma x)\left(\int_{A'_M/A_G(}\right.$$

a formula which holds whenever $\mathcal{T}$ satisfies the c

4. Counting lattice points

For each reduced root β of (G, A_{M_0}), we have the
an element in the lattice

$$X_*(A_{M_0})=\mathrm{Hom}(X(A_{M_0}),\mathbb{Z})$$

in $\mathbf{a}_{M_0}$. Suppose that $P\in\mathcal{P}(M)$ and that α is a roo
with $P_0\subset P$, there is a unique root $\beta\in\Delta_{P_0}$ whos
"co-root" $\alpha^\vee\in\Delta_P^\vee$ is, by definition, the projection
in $\mathbf{a}_M^G$, generated by $\Delta_P^\vee$, is the projection of $\mathbb{Z}(\Delta_{P_0}^\vee)$ o
of P_0, $\mathbb{Z}(\Delta_P^\vee)$ is independent of P. The lattice $\mathbb{Z}(\Delta_

$$X_*(A_M)=\mathrm{Hom}(X(A_M),\mathbb{Z}).$$

However, it is easily seen to be a subgroup of

$$\mathrm{Hom}(X(M)_F,\mathbb{Z}),$$

which is in turn a finite extension of $X_*(A_M)$. Cons
that $k\mathbb{Z}(\Delta_P^\vee)$ is a subgroup of $X_*(A_M)$.

Recall that

$$\exp(\langle H_M(m),\chi\rangle)=|\chi(m)|,$$

for any $\chi\in X(M)_F$ and $m\in M(F)$. It follows easily t

is a subgroup of finite index in $A_M(F)$; it is this group which we v formula (13). The first step will be to calculate the integral

$$\int_{A'_{M,k}/A_G(F)} \sigma_M(H_M(a), \mathscr{Y}(x, \mathscr{T}))\mathrm{d}a.$$

The kernel of H_M in $A'_{M,k}$ equals the group

$$\kappa_M = A_M(F) \cap K.$$

It follows easily that the quotient of $A'_{M,k}/A_G(F)$ by κ_M/κ_G is isom to $\Lambda_{M,k}$. We can therefore write (14) as the product of the volume number of points in the intersection of $\Lambda_{M,k}$ with $S_M(\mathscr{Y}(x, \mathscr{T}))$. Conse be rewritten as

$$\mathrm{vol}(\kappa_M/\kappa_G) \lim_{\lambda \to 0} \left\{ \sum_{\xi} e^{\lambda(\xi)} \right\},$$

the sum being taken over ξ in $\Lambda_{M,k} \cap S_M(\mathscr{Y}(x, \mathscr{T}))$. We shall calc method in ([1], § 3).

Take λ to be a point in $\mathbf{a}^*_{M,\mathbb{C}}$ whose real part $\lambda_{\mathbb{R}} \in \mathbf{a}^*_M$ is regula shall write

$$\Delta^{\lambda}_P = \{\alpha \in \Delta_P : \lambda_{\mathbb{R}}(\alpha^{\vee}) < 0\}.$$

Let ϕ^{λ}_P denote the characteristic function of the set of $H \in \mathbf{a}_M$ such t each $\alpha \in \Delta^{\lambda}_P$, and $\varpi_{\alpha}(H) \leqslant 0$ for any α in the complement of Δ^{λ}_P in Δ

$$\hat{\Delta}_P = \{\varpi_{\alpha} : \alpha \in \Delta_P\}$$

is the basis of $(\mathbf{a}^G_M)^*$ which is dual to $\{\alpha^{\vee} : \alpha \in \Delta_P\}$.) It follows easily combinatorial lemma that

$$\sum_{P \in \mathscr{P}(M)} (-1)^{|\Delta^{\lambda}_P|} \phi^{\lambda}_P(H - Y_P(x, \mathscr{T})), \quad H \in \mathbf{a}_M,$$

equals the characteristic function of $S_M(\mathscr{Y}(x, \mathscr{T}))$ (See Lemma 2

for positive numbers t_α, with $0 < t_\alpha \leqslant 1$. The set (17) can t

$$\left\{ Y_P^\lambda + \sum_{\alpha \in \Delta_P^\lambda} n_\alpha \mu_{\alpha,k} - \sum_{\alpha \in \Delta_P - \Delta_P^\lambda} n_\alpha \mu_{\alpha,k} \right\},$$

where each n_α ranges over all positive integers. Expressio
geometric series, which equals

$$(-1)^{|\Delta_P^\lambda|} \exp[\lambda(Y_P^\lambda)] \prod_{\alpha \in \Delta_P^\lambda} (1 - \exp[\lambda(\mu_{\alpha,k})])^{-1} \prod_{\alpha \in \Delta_P}$$

If $\lambda_{\mathbb{R}}$ belongs to the negative chamber $-(\mathbf{a}_P^*)^+$ of P in $\mathbf{a}_M^*$, w

$$Y_P^+ = Y_P(x, \mathscr{T})^+ = (T_P - H_{\bar{P}}(x))^+.$$

Then for general λ,

$$Y_P^+ = Y_P^\lambda + \sum_{\alpha \in \Delta_P - \Delta_P^\lambda} \mu_{\alpha,k}.$$

Expression (16) may therefore be written as

$$\exp[\lambda(Y_P^+)] \prod_{\alpha \in \Delta_P} (\exp[\lambda(\mu_{\alpha,k})] - 1)^{-1}.$$

We have shown that (14) equals

$$\operatorname{vol}(\kappa_M/\kappa_G) \lim_{\lambda \to 0} \sum_{P \in \mathscr{P}(M)} (\exp[\lambda(Y_P^+)] \prod_{\alpha \in \Delta_P} (\exp[\lambda(\mu$$

Let us rewrite this last formula for (14) as

$$\operatorname{vol}(\kappa_M/\kappa_G) \lim_{\lambda \to 0} \sum_{P \in \mathscr{P}(M)} c_P(\lambda, x, \mathscr{T}) d_P(\lambda) \theta_P(\lambda)^{-1},$$

where

$$c_P(\lambda, x, \mathscr{T}) = \exp[\lambda(Y_P^+)] = \exp[\lambda((T_P - H_{\bar{P}}(x)$$

This follows the notation of ([3], § 6). In particular,

$$c_M^Q(x, \mathscr{T}) = \lim_{\lambda \to 0} \sum_{\{P \in \mathscr{P}(M): P \subset Q\}} \exp[\lambda((T_P - H_{\bar{P}}(x))^+)] \theta_P(\lambda)^{-1}$$

Next, we substitute the formula we have just established for (14) (13). We see that $\Theta_\pi(f)\Theta_\pi(\gamma)$ equals

$$\mathrm{vol}(\kappa_M/\kappa_G) \sum_{Q \in \mathscr{F}(M)} d_Q' \int_{A_{M,k}' \backslash G(F)} f(x^{-1}\gamma x) c_M^Q(x, \mathscr{T}) \mathrm{d}x.$$

For any group $Q \in \mathscr{F}(M)$ we have

$$c_M^Q(x, \mathscr{T}) = c_M^Q(m_{\bar{Q}}(x), \mathscr{T}).$$

It follows easily from this fact that

$$\int_{A_{M,k}' \backslash G(F)} f(x^{-1}\gamma x) c_M^Q(x, \mathscr{T}) \mathrm{d}x$$

is a multiple of

$$\int_K \int_{N_{\bar{Q}}(F)} \int_{A_{M,k}' \backslash M_{\bar{Q}}(F)} f(k^{-1} m^{-1} \gamma m n k) c_M^Q(m, \mathscr{T}) \mathrm{d}m \, \mathrm{d}n \, \mathrm{d}k.$$

Since f is a supercusp form, this expression vanishes for any $Q \neq G$.

$$\Theta_\pi(f)\Theta_\pi(\gamma) = \mathrm{vol}(\kappa_M/\kappa_G) d_G' \int_{A_{M,k}' \backslash G(F)} f(x^{-1}\gamma x) c_M(x, \mathscr{T}) \mathrm{d}x$$

Now, by definition,

$$d_G' = d_G'(0) = \lim_{\lambda \to 0} d_P(\lambda),$$

for any $P \in \mathscr{P}(M)$. Therefore

since the map

$$A_M(F)/A'_{M,k} \to (H_M(A_M(F)) + \mathbf{a}_G)/(\Lambda_{M,k} + \mathbf{a}_G)$$

is an isomorphism. Our formula becomes

$$\Theta_\pi(f)\Theta_\pi(\gamma) = |A_M(F)/A'_{M,k}|^{-1} \int_{A'_{M,k}\backslash G(F)} f(x^{-1}$$

It is valid whenever $\mathscr{T}$ satisfies the conditions (8)

5. Completion of the proof

The formula (19) is close to that of the theorem. The or
on $(T_P - H_{\bar{P}}(x))^+$, rather than the vector $T_P - H_{\bar{P}}(x)$.
average $\mathscr{T}$ over a certain compact domain.

Observe that $\Lambda_{M,k}$ is the projection onto $\mathbf{a}_M^G$ of the l

$$\Lambda_{M_0,k} = k \log(q_F)\mathbb{Z}(\Delta_{P_0}^\vee), \quad P_0 \in \mathscr{P}(M_0),$$

in $\mathbf{a}_{M_0}^G$. Choose an element P'_0 in $\mathscr{P}(M_0)$, and let $\mathscr{D}$ den
domain

$$\left\{ u = \sum_{\beta \in \Delta_{P'_0}} u_\beta \mu_{\beta,k} \cdot 0 \leqslant u_\beta \leqslant 1 \right\}$$

for $\Lambda_{M_0,k}$ in $\mathbf{a}_{M_0}^G$. (Recall that $\{\mu_{\beta,k}\}$ is a basis of $\Lambda_{M_0,k}$ c
of the co-roots $\Delta_{P'_0}^\vee$). Suppose that $P \in \mathscr{P}(M)$. Then th
that $P_0 = sP'_0$ contains P. For each $\alpha \in \Delta_P$, let $\beta(\alpha)$ be
that the restriction of $s\beta(\alpha)$ onto $\mathbf{a}_M$ equals α. Then μ_α
onto $\mathbf{a}_M$. Given a vector $u \in \mathscr{D}$ as above, set

$$u_P = \sum_{\alpha \in \Delta_P} u_{\beta(\alpha)} \mu_{\alpha,k}.$$

This is a product of two (G, M) families. We can therefore apply Le to decompose $c_M(x, \mathscr{T}_u)$ into a sum over $Q \in \mathscr{F}(M)$. The second (independent of x. By arguing as in § 4, we see that the contribution c the integral

$$\int_{A'_{M,k}\backslash G(F)} f(x^{-1}\gamma x) c_M(x, \mathscr{T}_u) \mathrm{d}x$$

vanishes. We may therefore replace $c_M(x, \mathscr{T}_u)$ by $c_M(x, \mathscr{T}, u)$, the term to $Q = G$. Since this is valid for any $u \in \mathscr{D}$, we may integrate over $\mathscr{D}$ follows that (19) remains valid if the function $c_M(x, \mathscr{T})$ is replaced by

$$\int_{\mathscr{D}} c_M(x, \mathscr{T}, u) \mathrm{d}u.$$

Now,

$$\int_{\mathscr{D}} c_M(x, \mathscr{T}, u) \mathrm{d}u$$

$$= \int_{\mathscr{D}} \lim_{\lambda \to 0} \sum_{P \in \mathscr{P}(M)} (c_P(\lambda, x, \mathscr{T}, u)\, \theta_P(\lambda)^{-1}) \mathrm{d}u$$

$$= \lim_{\lambda \to 0} \sum_{P \in \mathscr{P}(M)} \left(\int_{\mathscr{D}} c_P(\lambda, x, \mathscr{T}, u) \mathrm{d}u \right) \theta_P(\lambda)^{-1}.$$

Thus, we have only to compute

$$\int_{\mathscr{D}} E((Y_P - u_P)^+ + u_P) \mathrm{d}u,$$

where

$$E((Y_P - u_P)^+ + u_P) = \exp[\lambda((Y_P - u_P)^+ + u_P)],$$

with

where $0 < t_\alpha \leqslant 1$. Taking the integrals in r_α separat
and $[1 - t_\alpha, 1]$, we can change variables; we obtain

$$E\left(Y_P + \sum_\alpha r_\alpha \mu_{\alpha,k} \right).$$

It follows that (20) equals

$$\int_{\mathscr{D}} E(Y_P + u_P) \mathrm{d}u.$$

We have shown that

$$\int_{\mathscr{D}} c_M(x, \mathscr{T}, u) \mathrm{d}u = \int_{\mathscr{D}} \bar{v}_M(x, \mathscr{T}, u) \mathrm{d}u,$$

where

$$\bar{v}_P(\lambda, x, \mathscr{T}, u) = \exp[T_P + u_P - H_{\bar{P}}(x)]$$

$$= \exp[-\lambda(H_{\bar{P}}(x))] \exp[\lambda(T_P$$

This is again a product of (G, M) families. We appl
and decompose $\bar{v}_M(x, \mathscr{T}, u)$ into a sum over $Q \in \mathscr{P}(M$
is independent of x, the contribution of any $Q \neq G$

$$\int_{A'_{M,k} \backslash G(F)} f(x^{-1} \gamma x) \int_{\mathscr{D}} \bar{v}_M(x, \mathscr{T}, u) \mathrm{d}u \mathrm{d}x = \int_{\mathscr{D}}$$

vanishes. The term corresponding to $Q = G$ is just

$$\bar{v}_P(\lambda, x) = \exp[-\lambda(H_{\bar{P}}(x))], \quad P \in \mathscr{P}(M).$$

This is of course independent of u, so the integral
(19) becomes

$$= (-1)^{\dim(A_M/A_G)} \sum_{P \in \mathscr{P}(M)} \exp[-\lambda(H_P(x))]\theta_P(\lambda)^{-1}$$

$$= (-1)^{\dim(A_M/A_G)} v_M(x),$$

since

$$\theta_{\bar{P}}(\lambda) = (-1)^{\dim(A_M/A_G)}\theta_P(\lambda).$$

In other words, $\Theta_\pi(f)\Theta_\pi(\gamma)$ equals

$$|A_M(F)/A'_{M,k}|^{-1}(-1)^{\dim(A_M/A_G)} \int_{A'_{M,k}\backslash G(F)} f(x^{-1}\gamma x) v_M(x)\mathrm{d}x$$

Now, it is well known that the function $v_M(x)$ is left invariant under M the integrand is left invariant under $A_M(F)$. We may therefore cha integration to $A_M(F)\backslash G(F)$, if we multiply by the index $|A_M(F)/A'_M$ identity of $\Theta_\pi(f)\Theta_\pi(\gamma)$ with

$$(-1)^{\dim(A_M/A_G)} \int_{A_M(F)\backslash G(F)} f(x^{-1}\gamma x) v_M(x)\mathrm{d}x.$$

This completes the proof of the theorem. □

References

[1] Arthur J, The characters of discrete series as weighted orbital integrals, *Invent. M*

[2] Arthur J, A trace formula for reductive groups I: terms associated to classes i **45** (1978) 911–952

[3] Arthur J, The trace formula in invariant form, *Ann. Math.* **114** (1981) 1–74

[4] Arthur J, On a family of distributions obtained from Eisenstein series II: Ex *Math.* **104** (1982) 1289–1336

[5] Harish-Chandra, *Harmonic analysis on reductive p-adic groups, Lecture Notes in* Heidelberg: Springer Verlag) (1970)

[6] Waldspurger J L, A propos des integrales orbitales pour $GL(N)$, preprint

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 21–30
© Printed in India.

On the proof of the reciprocity law for arithmetic Siegel modular functions*

WALTER L BAILY Jr

Department of Mathematics, The University of Chicago, 5734 Uni
Chicago, Illinois 60637, USA

Abstract. Earlier we obtained a new proof of Shimura's reciprocity l
of arithmetic Hilbert modular functions. In this note we show how
derive Shimura's reciprocity law for special values of arithmetic Si
To achieve this we use Shimura's classification of the special poi
Satake's classification of the equivariant holomorphic imbeddings of
spaces into a larger Siegel space, and, finally, a corrected version o
giving an action of the Galois group $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$ on arithmetic Sie

Keywords. Reciprocity law; arithmetic Siegel modular functions; Si

1. Introduction

In [5] we obtained a new proof of Shimura's reciprocity law [
values of certain arithmetic Hilbert modular functions. In this
from this result one may derive the reciprocity law for special
Siegel modular functions as formulated in [16]. To achieve thi
results classifying the special points of the (adelized) Siegel spa
classifying the equivariant holomorphic imbeddings of a produc
modular spaces into a larger Siegel space, and, finally, a corre
Karel's results [6] giving an action of the Galois group $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$
modular forms which commutes with translation in the finite adele

$(x, \xi) \to x * \xi$, $\xi \in \Xi$, $x \in \mathbf{I}(K)$, of the ideles $\mathbf{I}(K)$ of K on
Suppose that $(\tau) = (\tilde{\sigma}_1(\tau), \ldots, \tilde{\sigma}_n(\tau)) \in \mathfrak{H}^n$ is the "infinite
be the *CM*-dual of $(K, \tilde{\Sigma})$ and $N_{\tilde{\Sigma}*}$ be the type no
$\mathbf{I}(K)$. One defines the notion of arithmetic Hilbert
main result of [5] is then

Theorem. *Let Φ be an arithmetic Hilbert modular f
Then in the above notation, one has the relation*

$$\Phi(N_{\tilde{\Sigma}*}(a) * \xi) = \mathfrak{a}(a) \cdot \Phi(\xi), \; a \in \mathbf{I}(K^*(\tilde{\Sigma})),$$

where $\mathfrak{a}$ is the Artin symbol, $\mathfrak{a}(a) = [a, K^*(\Sigma)]$.

This result, due originally to Shimura [14], wa
methods. In the present article, we shall sketch how
directly the reciprocity law for arithmetic Siegel m
state later on, and which is essentially that obtaine

2. Classification of special points on the Siegel spac

Denote by $\mathfrak{S}_n$ the Siegel upper half space of degree
symmetric matrices $Z = X + iY$ such that Y is posi
the $2n$ by $2n$ skew-symmetric matrix

$$\begin{bmatrix} 0 & 1_n \\ -1_n & 0 \end{bmatrix}.$$

The group $Gp(n, \mathbf{R})$ of symplectic similitudes, defin

$$Gp(n, \mathbf{R}) = \{X \in M_{2n}(\mathbf{R}) \mid {}^tX \cdot J_n \cdot X = \nu(X) \cdot$$

contains the normal subgroup $Gp^+(n, \mathbf{R})$ of index
$\nu(X) > 0$, and the latter group acts transitively on

direct sum of simple algebras

$$Y = Y_1 \oplus \cdots \oplus Y_t,$$

each Y_j is stable under ρ, and, as we shall see, is a total matric a
CM-field K_j, with maximal totally real subfield denoted by k_j. Z
the centre of Y, and the fixed algebra of ρ in Z is $Z_0 = k_1 \oplus \cdots \oplus$
the unique isolated fixed point of the group

$$Z_1 = \{z \in Z \mid zz^\rho = \mathbf{1}_{2n}\} \subset Z^\times.$$

Let $m_j = [k_j:\mathbf{Q}]$ and $q_j^2 = \dim_{K_j} Y_j$. In the present case, the totally r
is just $\mathbf{Q}$ and the quaternion algebra B over F is $M_2(\mathbf{Q})$. Hence
which has to be in the same Brauer class over K_j as $B \otimes_{\mathbf{Q}} K_j$ [15:§
total matric algebra over K_j and $Y_j \cong M_{q_j}(K_j)$. We have inclusion

$$K_j \longrightarrow M_2(k_j) \longrightarrow M_{2m_j}(\mathbf{Q})$$

coming from the regular representation of K_j as an algebra over
$\mathbf{Q}$-algebra; thus we also have

$$Y_j = M_{q_j}(K_j) \longrightarrow M_{2n_j}(\mathbf{Q}), \quad n_j = m_j q_j,$$

and $n = n_1 + \cdots + n_t$. Moreover, the centralizer $\mathfrak{C}(\xi)$ of Z_0 in M_2
matric algebra defined over $\mathbf{Q}$) is the direct sum over j of the cent
M_{2n_j}, $j = 1, \ldots, t$. The centralizer of k_j in M_{2n_j} (as an algebraic to
over $\mathbf{Q}$) is just $R_{k_j/\mathbf{Q}} M_{2q_j}$, so that

$$\mathscr{Z}_j(\mathbf{Q}) \cong M_{2q_j}(k_j).$$

Then the centralizer of Z_0 in Sp_n is the direct product

$$\prod_{j=1}^{t} R_{k_j/\mathbf{Q}} Sp_{q_j} \longrightarrow Sp_n;$$

and if we let $G_j = R_{k_j/\mathbf{Q}} Sp_{q_j}$, $K_{j1}{}^\times = \{\alpha \in K_j \mid \alpha\bar{\alpha} = 1\}$, then we have a

morphism f, of the special point

$$(\xi_1, \ldots, \xi_t) \in (\mathfrak{S}_{q_1})^{m_1} \times \cdots \times (\mathfrak{S}_{q_t})^{m_t}.$$

That equivariant holomorphic morphism comes from

$$\varphi: G_1 \times \cdots \times G_t \longrightarrow Sp_n$$

of algebraic groups, all defined over $\mathbf{Q}$. It is clear from φ satisfies not only the condition (H_1), but also (H_2) extension of f carries the 0-dimensional (point) rational product

$$\prod_j (\mathfrak{S}_{q_j})^{m_j}$$

into 0-dimensional rational boundary components of

Next one needs to consider the special point ξ_j on th it in turn is the image of a special point on a product type" as considered in [5]. For this, we temporarily fi and let K be a CM-field with maximal totally real subf for a positive integer q, form the group $G'' = R_{k/\mathbf{Q}} Sp_q$, so $\mathfrak{S}_q{}^m$, and any subgroup of it commensurable with the of degree q over k[1, 10] acts discontinuously on this this special case) $Y = M_q(K)$ and $G = R_{k/\mathbf{Q}} Sp_q$.

Let $K_1{}^\times = \{\alpha \in K \mid \alpha\bar{\alpha} = 1\}$, $Y = Y(\xi) \cong M_q(K)$ provide δ defined by $y^\delta = {}^t y^i$ in the notation of [15, §4]; the group of $\mathbf{Q}$-rational points of the maximal compa $\xi = (\xi^{(1)}, \ldots, \xi^{(m)}) \in \mathfrak{S}_q{}^m$. We have

$$K_1{}^\times \longrightarrow Y_1 \longrightarrow (R_{k/\mathbf{Q}} Sp_q)(\mathbf{Q}),$$

and $\xi^{(i)}$ is the unique fixed point of $K_1{}^\times$ acting thus on power $\mathfrak{S}_q{}^m$, $i = 1, \ldots, m$. In other words, for each $i = 1$,

$w_\nu = v_\nu + \bar{v}_\nu$ and $w_\nu' = (-D)^{-1/2}(v_\nu - \bar{v}_\nu)$ (where $D \in k$ is totally
$K = k(\sqrt{-D})$). Thus, $W_\nu = \mathbf{R}w_\nu + \mathbf{R}w_\nu'$ is a real hyperbolic plane
restriction of A and W_ν is defined over k. Choosing $v_1, \ldots, v_q$ in
assume that v_ν is orthogonal to the complex conjugates of $v_{\nu'}$ for
hence that the hyperbolic planes W_ν are mutually orthogonal v
skew-symmetric form A. In this way we obtain an *orthogonal* dec

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_q$$

of V into mutually orthogonal hyperbolic planes defined over
inclusions of k-groups

$$K_1^{\times} \longrightarrow SL(W_1) \times \cdots \times SL(W_q) \longrightarrow Sp(V, A),$$

where the first imbedding on the left comes from the facts that
eigenvectors of $K_1^{\times}$ and W_ν is rational over k and where the secon
comes from an isometry of symplectic spaces of $W_1 \oplus W_2 \oplus \cdots$
application of the groundfield reduction functor $R_{k/\mathbf{Q}}$, we further
of imbeddings

$$K_1^{\times} \longrightarrow R_{k/\mathbf{Q}}SL_2 \times \cdots \times R_{k/\mathbf{Q}}SL_2 \longrightarrow R_{k/\mathbf{Q}}Sp_q.$$

Now let $G_1 = R_{k/\mathbf{Q}}SL_2$, $G_2 = R_{k/\mathbf{Q}}Sp_q$. We obtain thus a diagram

$$\begin{array}{ccc} K_1^{\times} \longrightarrow G_1(\mathbf{R}) \times \cdots \times G_1(\mathbf{R}) & \longrightarrow & G_2(\mathbf{R}) \\ \downarrow \qquad\qquad\qquad \downarrow & & \downarrow \\ \mathfrak{H}^m \times \cdots \times \mathfrak{H}^m & \longrightarrow & \mathfrak{S}_q^m, \ \mathfrak{H} = \mathfrak{S}_1, \end{array}$$

such that under the mapping of the lower line, the special point (
product on the left is mapped to the special point $\xi \in \mathfrak{S}_q^m$, where $\xi($
of the ν-th factor with respect to an imbedding of $K_1^{\times}$ in $G_1(\mathbf{R})$, G_1 ca
such that all the Hilbert modular subgroups of $SL_2(k)$ are containe
that $K_1^{\times} \to G_1(\mathbf{Q})$ is an imbedding of the group of $\mathbf{Q}$-points of an $\mathbf{R}$

Combining this discussion with the preceding observations, an

spaces. Let H_j be the direct product of G_m and S_j. The homor properties which we now describe.

First of all, any two such φ' (for the same $k_1, \ldots, k_s$) are c of $Sp(n, \mathbf{Q})$, since both are induced by isometries into the symp it is easy to see that φ' and f' satisfy Satake's conditions particular the extension of f' to the Satake compactification the projective limit of Satake compactifications with respect t groups commensurable with the respective Hilbert modular point boundary components of the left side to rational point of the right side. Thus, by a suitable choice of coordinates on suppose that f' is a *linear* mapping with coefficients that a sense (i.e. with respect to the given **Q**-structures).

3. The homomorphism of the graded algebra of (arithmetic)

In [4] we have already introduced a notion of arithmetic mo group of $R_{k/\mathbf{Q}}GL_2$, where k is a totally real field, and used this stated above of Shimura's reciprocity law for Hilbert modula is based on the theory of the Fourier expansions of Eisens group. In [6] Karel has introduced a similar but more gene modular form on the adele group of an algebraic group wh rational symmetric tube domain. Though there is an error i subsequently corrected that [7], and proposes to publish th a larger undertaking . We subsume here that portion of his necessary for our purposes. Namely, on the graded algebra the adele group of the group Gp_n of symplectic similitudes d introduce a $\mathbf{Q}_{ab}$-structure and an operation of the Galois gr $\mathscr{A}$ which commutes with translation by elements of $Gp_n(\mathbf{A}_f)$, th $\mathbf{A} = \mathscr{A}^{\mathscr{G}}$ determines the **Q**-structure on $\mathscr{A}$. The field of ho degree zero of **A** is denoted by **M** and is called the field of arithm

To describe the action of $\mathscr{G}$ on $\mathscr{A}$ and define the **Q**-arithm functions, we recall [7] the existence of a certain **Q**-rational ho

open compact subgroup $\mathbf{K}$ of $G(\mathbf{A}_f)$, then f has a Fourier exp
distinguished point ∞ at infinity corresponding to P on eac
$G(\mathbf{A})/\mathbf{K}_\infty\mathbf{Z}^-$, where $\mathbf{Z}^-$ is the closure of $Z(\mathbf{Q})_f$ in $G(\mathbf{A}_f)$. Then if $\tau\in$
on the Fourier coefficients of each of these Fourier expansions (wh
lie in $\mathbf{Q}_{ab}$), one obtains the set of Fourier expansions of a $\mathbf{Q}_{ab}$-ar
form $\tau * f$ with respect to $\mu(\tau)_\mathbf{K} = \mu(\tau)\mathbf{K}\mu(\tau)^{-1}$, hence if R denotes ri
$G(\mathbf{A})$, f^τ defined by

$$f^\tau(x) = (R(\mu(\tau)^{-1})\cdot(\tau * f))(x) = (\tau * f)(x\mu(\tau)^{-1}), \quad x\in G(\mathbf{A}),$$

is a modular form in $\mathscr{A}(\mathbf{K}, \mathbf{Q}_{ab})$. If we define thus the action of $\mathscr{G}$
the set $\mathbf{A} = \mathscr{A}^\mathscr{G}$ of invariants of $\mathscr{G}$ defines a $\mathbf{Q}$-structure on $\mathscr{A}$, an
called $\mathbf{Q}$-arithmetic modular forms. The homogeneous quotients
$(f/g, f, g\in\mathbf{A}_m, g\neq 0)$ are called $\mathbf{Q}$-arithmetic modular functions.

When $G = R_{k/\mathbf{Q}}GL_2$, k totally real, define $\mu'\colon G_m \to GL_2 : s \to \mathrm{diag}($
to conjugacy over $GL_2(k)$), and

$$\mu = R_{k/\mathbf{Q}}\mu'\colon G_m \longrightarrow G = R_{k/\mathbf{Q}}GL_2.$$

When $k = k_j$, denote μ (resp. G) by μ_j (resp. G_j). Let H be the alge
$G = \prod_j G_j$ generated by the subgroups $S = \prod_j S_j$ and $\mu(G_m)$, where μ:
as $\prod_j \mu_j$. Then H is the direct product of S and $\mu(G_m)$, and contai
the direct product H_j of S_j and $\mu(G_m)$, which is isomorphic over $\mathbf{Q}$
Then the homomorphism $Z_1 = \prod_j {K_{j1}}^\times \subset\!\!\to Sp_n$ is factored by way

$${K_{j1}}^\times \subset\!\!\to S_j \subset\!\!\to Sp_n, \quad j = 1, \ldots, s;$$

and $\mu\colon G_m \to Gp_n$ is factored by way of H_j:

$$G_m \xrightarrow{\mu} H \xrightarrow{\varphi'} Gp_n,$$

where φ' satisfies (H_2) and (H_2'). Now $\mathbf{Q}$-arithmetic modular form
on $H(\mathbf{A})$ alone, since $H(\mathbf{A})$ is invariant under translation by $\mathrm{diag}(s,$

4. Action of the ideles of the composite K* of the refle special points of $Gp_n(\mathbf{A})$

Now let $G' = Gp_n(\mathbf{A}), G = \prod_j G_j$, and let

$$\xi \in V'_\infty = G'(\mathbf{A})/\mathbf{K}_\infty \mathbf{Z}^- = \varprojlim_{\mathbf{K}} V'_{\mathbf{K}}, \quad V'_{\mathbf{K}} = G'($$

be a special point; for simplicity of notation we may (*wi* $\xi \in \mathfrak{S}_n$ is a special point with respect to the action of S we have observed above, there exists an imbedding d groups defined over $\mathbf{Q}$ into Sp_n:

$$R_{k_1/\mathbf{Q}} SL_2 \times \cdots \times R_{k_s/\mathbf{Q}} SL_2 \hookrightarrow Sp_n,$$

where $[k_i:\mathbf{Q}] = n_i$, $i = 1, \ldots, s$, and $n = n_1 + \cdots + n_s$, s imbedding of rational tube domains,

$$\mathfrak{H}^{n_1} \times \cdots \times \mathfrak{H}^{n_s} \longrightarrow \mathfrak{S}_n,$$

the special point ξ is the image of $(\xi_1, \ldots, \xi_s)$, where ξ_j respect to the action of S_j. Let K_j be the CM-field associated to the special point $\xi_j \in \mathfrak{H}^{n_j}$ on which $(R_{k_j/\mathbf{Q}}G$ its CM-dual. Now if Φ_j is an arithmetic modular functi to an open compact subgroup $\mathbf{K}_j$ of $R_{k_j/\mathbf{Q}} GL_2(\mathbf{A})$, regu

$$K_j^*(\Phi_j(\xi_j))/K_j^*$$

is an abelian extension with reciprocity law given by

$$[v, K_j^*] \cdot \Phi_j(\xi_j) = \Phi_j(v * \xi_j), \quad v \in \mathbf{A}(K_j^*)^\times.$$

Let K^* be the compositum of the fields $K_1^*, \ldots, K_s^*$ extension of K^*, and if $v^* \in \mathbf{A}(K^*)^\times = \mathbf{I}(K^*)$, then ap special values of arithmetic Hilbert modular function the well-known properties of the Artin symbol, one c

$$V_{\mathbf{K}} = G_+(\mathbf{Q})\backslash G_+(\mathbf{A})/\mathbf{K}\mathbf{K}_{\infty}, \quad \mathbf{K} = \prod_{j=1,\ldots,s} \mathbf{K}_j,$$

where $\mathbf{K}_j$ is open, compact in $G_j(\mathbf{A}_f)$.

Let A be an affine $\mathbf{Q}$-open subset of $V_{\mathbf{K}}$ containing the image ir
of the special point $(\xi) = (\xi_1, \ldots, \xi_s)$ under the group $\mathbf{I}(K^*)$ as ex
is possible since V is defined over $\mathbf{Q}$ and the image of that orbi
$V_j = G_{j+}(\mathbf{Q})\backslash G_{j+}(\mathbf{A})/\mathbf{K}_j\mathbf{K}_{\infty,j}$, where $\mathbf{K}_{\infty,j}$ has a meaning for $G_{j+}(\mathbf{R})$
of $\mathbf{K}_{\infty}$ for $G_+(\mathbf{R})$.

As before, let H be the algebraic group $\mu(G_m)\cdot\prod_j S_j$ which is de
$\mu(G_m)$ is defined with respect to the maximal torus T defined by

$$T = Z'\cdot\prod_j R_{k_j/\mathbf{Q}} T_j'',$$

T_j'' being a k_j-split maximal torus of SL_2 defined over k_j, and Z
G. (Then $T_j' = R_{k_j/\mathbf{Q}} T_j''$ is a maximal torus of maximal $\mathbf{Q}$-rank in S_j.

$H(\mathbf{A})$ is an open subgroup of $G(\mathbf{A})$, and its image $V_{\mathbf{K},H}$ in $V_{\mathbf{K}}$ is
of the latter and defined over $\mathbf{Q}$ for reasons noted earlier. If
modular form on $G'(\mathbf{A})$ ($G' = Gp_n$), then f may be pulled back to an
form f^* on $H(\mathbf{A})$. On the other hand, each of the groups $H_j =$
be viewed as imbedded in H, and f^* may be pulled back to H
easily seen, the reciprocity law for special values of Hilbert mo
applies to the restrictions $f_j = f^*|H_j$, $j = 1, \ldots, s$, and in the sam
in the Theorem stated in the introduction.

We may then assume the open affine set A is contained in $V_{\mathbf{K},H'}$
$i = 1, \ldots, N_j\}$ be a system of generators of the affine coordina
$A \cap (V_{\mathbf{K}_1} \times \cdots \times V_{\mathbf{K}_j})$, where each Φ_{ji} is an arithmetic modular func
a $\mathbf{Q}$-arithmetic modular function Φ on $\mathfrak{S}_n$ whose pullback is regu
combination of products

$$\Phi_{1i_1}\Phi_{2i_2} \times \cdots \times \Phi_{si_s}$$

with rational coefficients. But the reciprocity law for such a prod
from what we have already done. Thus we have, in conclusion,

of upper half-planes, together with equivariant morphisms and a special point $(\xi_1, \ldots, \xi_s) \in \mathscr{P}$ *such that* $f(\xi_1, \ldots, \xi_s) =$

Let $\xi_{\mathbf{K}}$ *denote the image of* ξ *in*

$$V_{\mathbf{K}}' = Gp_n(\mathbf{Q}) \backslash Gp_n(\mathbf{A}) / \mathbf{K}' \mathbf{K}'_{\infty}.$$

Then, with $[\,,]$ *denoting the Artin symbol, we have*

$$[v^*, K^*] \cdot \Phi(\xi_{\mathbf{K}}) = [v^*, K^*] \cdot \Phi \circ f(\xi_1, \ldots, \xi_s)$$

$$= (\Phi \circ f)(N_{\tilde{\Sigma}_1 *}(N_{K^*/K_1 *} v^*) * \xi_1, \ldots, N_{\tilde{\Sigma}_s *}(N_{K^*/K}$$

(Note that the argument appearing in the function $\Phi \circ f$ special point of $V_{\infty} = G_+(\mathbf{Q}) \backslash G_+(\mathbf{A}) / \mathbf{Z}^- \mathbf{K}_{\infty}$ (with G as ab in $V_{\mathbf{K},H}$, and whose image under f is the image of a speci

It would seem that from this result one should be some of the main theorems for canonical models co thence, by imbeddings, for the canonical models connec be equivariantly imbedded in Siegel space.

References

[1] Baily W L Jr, On the Hilbert–Siegel modular space, *Am. J. Mat*

[2] Baily W L Jr, On the theory of Hilbert modular functions I, Arith *J. Algebra* **90** (1984) 567–605

[3] Baily W L Jr, Arithmetic Hilbert modular forms, *Proc. Int. Sym variables* (eds) Y Morita and I Satake (Boston: Birkhäuser) (1983

[4] Baily W L Jr, Arithmetic Hilbert modular functions **II** *Rev. Mat*

[5] Baily W L Jr, Reciprocity laws for special values of Hilbert modula *Workshop* (eds) J K Koo and D Y Suh (Korea: Taejon) (1986)

[6] Karel M, Eisenstein series and fields of definition, *Compos. Math*

[7] Karel M, Corrections to my paper 'Eisenstein series and fields of

[8] Karel M, Special values of elliptic modular functions, *Proc. Int. Sy variables* (eds) Y Morita and I Satake (Boston: Birkhäuser) (1983

[9] Karel M, Special values of Hilbert modular functions, *Rev. Mat.*

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 31–43.
© Printed in India.

On some generalizations of Ramanujan's continued frac

S BHARGAVA[†], CHANDRASHEKAR ADIGA[†] and
D D SOMASHEKARA*

[†]Department of Mathematics, Manasagangotri, University of Mysor
*Department of Mathematics, Yuvaraja's College, University of M
India

Abstract. In this note we establish continued fraction developments f
hypergeometric function ${}_2\phi_1(a, b; c; x)$ with several of its contiguo
generalize and give a unified approach to establishing several conti
including those of Srinivasa Ramanujan.

Keywords. q-continued fractions; Rogers-Ramanujan continued fra
metric series.

1. Introduction

In [6] Bhargava and Adiga established equivalents of the follow
fractions I and II which contain as special cases several continued
stated in the 'lost' notebook of Srinivasa Ramanujan [14] and
different methods by Andrews [2], [3], Bhargava and Adiga [5]
[11] and Ramanathan [12].

$$ {}_2\phi_1(a, b; c; xq)/{}_2\phi_1(a, b; c; x) = h(a, b, c, xq)(1 - x)/h(a, b, c$$

$$= \cfrac{1}{1 + \cfrac{x(1-a)(1-b)}{1 - x + \cfrac{abxq - c}{1 + \cfrac{x(1-aq^n)(1-bq^n)}{1 - x + \cdots}}}}$$

with

$$(c)_\infty = \prod_{n=0}^{\infty} (1 - cq^n), \quad (c)_k = \frac{(c)_\infty}{(cq^k)_\infty} \quad (k: \text{in}$$

The purpose of this paper (§3) is to establish i more continued fraction expansions of the r ${}_2\phi_1(a, b; c; xq)/{}_2\phi_1(a, b; c; x)$, ${}_2\phi_1(aq, b; c; x)/{}_2\phi_1(a, b;$ ${}_2\phi_1(a, b; cq; xq)/{}_2\phi_1(a, b; c; x)$, ${}_2\phi_1(aq, b; c; x/q)/{}_2\phi$ $(a, b; c; x)$, ${}_2\phi_1(a, bq; cq; x)/{}_2\phi_1(a, b; c; x)$. ${}_2\phi_1(aq,$ obtain some identities of Ramanujan [4], [13], as special cases. Denis [7] has recently given an al Andrews [2].

In §2 we obtain some easily verified functional r function h given by (2). These functional relations at Thus, the use of h considerably simplifies and brings that (2) immediately gives the symmetry

$$h(a, b, c, x) = h(b, a, c, x), \quad |q| < 1, \quad |x| <$$

The well-known E Heine's transformation satisfie

$$h(abx/c, b, bx, c/b) = h(a, b, c, x), \quad |q| < 1$$

Further, changing

$$a \text{ to } -\lambda/a, \quad b \text{ to } c, \quad c \text{ to } -bq \quad \text{and}$$

the function h is easily seen to be the same as the fu proving I and II. We indicate some special cases i

2. Some functional relations satisfied by h

Lemma 2.1. The function h given by (2) satisfies

terms from other terms, becomes

$$(x)_\infty(cq)_\infty\left[-c+\sum_{n=1}^{\infty}\frac{(a)_n(b)_n x^n}{(q)_n(cq)_n}(1-cq^n-1)\right]$$

$$=-c(x)_\infty(cq)_\infty\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(q)_n(cq)_n}(xq)^n$$

which equals the right side of (7). Now, the left side of (8) can b

$$(c)_\infty(xq)_\infty\left[(1-x)\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n(q)_n}x^n-\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n(q)_n}x^nq^n\right]$$

$$=(c)_\infty(xq)_\infty\left[\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n(q)_n}x^n-\sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n(q)_n}x^{n+1}-\sum_{n=0}^{\infty}\right.$$

$$=(c)_\infty(xq)_\infty\left[\sum_{n=1}^{\infty}\frac{(a)_n(b)_n}{(c)_n(q)_{n-1}}x^n-\sum_{n=1}^{\infty}\frac{(a)_{n-1}(b)_{n-1}}{(c)_{n-1}(q)_{n-1}}x^n\right.$$

On combining the first and third summations,

$$=x(cq)_\infty(xq)_\infty\sum_{n=1}^{\infty}\frac{(a)_{n-1}(b)_{n-1}}{(cq)_{n-1}(q)_{n-1}}x^{n-1}X$$

where $X=(-aq^{n-1}-bq^{n-1}+cq^{n-1}+abq^{2n-2})$, which, on spli
mations, is easily seen to equal the right side of (8).

We need the following additional functional relations.

Lemma 2.2. The function h given by (2) satisfies

$$h(a,b,c,x)-(1-x)h(a/q,b,c,xq)=x(1-b)h(a,bq,cq,$$

$$h(a,b,c,x)-h(a/q,bq,c,x)=x((a/q)-b)h(a,bq,cq,x),$$

$$h(a,b,c,x)-h(a,bq,cq,(x/q))=((ax/q)-c)h(a,bq,cq,$$

then changing abx/c to A, b to B, bx to C and c/b to X; a
X as a, b, c and x respectively.

Identity (12) follows from (2) on using the two easil

$$(a)_n - (aq)_n q^{-n} = \begin{cases} 0 & , \quad n \\ -q^{-n}(aq)_{n-1}(1-q^n), & n \end{cases}$$

$$\frac{(b)_n}{(c)_n} - \frac{(b)_{n-1}}{(c)_{n-1}} = \frac{q^{n-1}(b)_{n-1}(c-b)}{(c)_n}, \quad n > 0.$$

3. Continued fraction developments

As shown in [6], I and II follow from the functional
Lemmas 3.1 and 3.2 below. We only indicate here how t
and (11).

Lemma 3.1.

$$h(a,b,c,x) = (1-x)h(a,b,c,xq) + x(1-a)(1$$

$$h(a,b,c,x) = h(aq,bq,cq,(x/q)) + (abx-c)h($$

Proof. Change a to aq in (9) and add the resulting equa
to aq in (11) and add to (6) to get (14).

Theorem 3.1. *Identity* I *of* § 1 *holds.*

Proof. See [6]

Lemma 3.2.

$$(1-x)h((a/q),b,c,xq) = \left[(1-c+bx) + \frac{x}{q}(\right.$$

Proof. Change a to (a/q), x to xq in (6) and multiply the result by $(1-x)$; in (11) and multiply the result by $(1-x)$; take the negative of (11); a equations to (9) to get (16).

Theorem 3.3.

$$\frac{{}_2\phi_1(a,b;c;xq)}{{}_2\phi_1(a,b;c;x)} = \frac{(1-x)h(a,b,c,xq)}{h(a,b,c,x)} = \frac{(1-x)}{K_0+}\,\frac{L_1}{K_1+\cdots}\,\frac{L_n}{K_n+\cdots}$$

where

$$K_n = 1 + \frac{c}{q} - (a+b)xq^n, \qquad n = 0,1,2,\ldots$$

$$L_n = \left(abxq^{n-1} - \frac{c}{q}\right)(1-xq^n), \quad n = 1,2,\ldots.$$

Proof. Changing b to (b/q), c to (c/q), x to xq^{n+1}, (16) can be written

$$W_n \equiv \frac{h(a,b,c,xq^n)}{h(a,b,c,xq^{n+1})} = K_n + \frac{L_{n+1}}{W_{n+1}}.$$

Iterating this with $n = 0, 1, 2, \ldots$ and taking the reciprocal and multiplyin have III.

Lemma 3.4.

$$\left(1-\frac{c}{bq}\right)h(a,b,c,x) = \left[\left(1-bx+\frac{c}{q}\right)\right.$$

$$\left. + b^{-1}q^{-2}(abxq - cq - c)\right]h(a,bq,c,x$$

$$- b^{-1}q^{-2}(-c+abxq)(1-bq)h(a,bq^2$$

Proof. Change b to bq^n in (17) and multiply the

$$T_n \equiv \frac{\left(q^n - \frac{c}{bq}\right)h(a, bq^n, c, x)}{h(a, bq^{n+1}, c, x)} = B_n + \frac{A}{T}$$

where, A_{n+1} and B_n are as above. Iterating the taking the reciprocal and using (2), we have III

Lemma 3.5.

$$h(a, b, c, x) = [1 - x(a + b - c)]h(a, b,$$
$$+ x(1 - xq)[ab - c(a +$$
$$h(a, b, c, xq) = [1 - xq(a + b) + c(xq^2$$
$$+ xq(1 - xq^2)[ab - cq($$

Proof. Changing x to xq in (7) and using the res have (18). Changing c to cq and x to xq in (18), c results we get (19).

Theorem 3.5.

$$\frac{{}_2\phi_1(a, b; c; xq)}{{}_2\phi_1(a, b; c; x)} = \frac{h(a, b, c, xq)(1 - x)}{h(a, b, c, x)}$$
$$= \frac{1 - x}{1 - x(a + b - c) +$$

where,

$$E_{n+1} = xq^n(1 - xq^{n+1})(a - cq^n)(b - c$$

Lemma 3.6.

$$h(a, bq, cq, (x/q)) = (1 - bx)h(a, bq, cq, x) + \frac{x}{q}(a - cq)(bq - 1)h(a, bq^2, cq^2, x),$$

$$h(a, b, c, xq) = (1 - c + ax - bxq)h(a, bq, cq, xq) + x(a - cq)(bq - 1)h(a, bq^2, cq^2, xq).$$

Proof. Change b to bq and c to cq in (9) and multiply the res
$(c - (ax/q))$; change a to (a/q), b to bq and c to cq in (6) and m
equation by $(1 - x)$; change a to (a/q) and x to xq in (11) and m
$(1 - x)$; take the negative of (11); and add all these equations to (9)
to xq in (22); change x to xq in (11) and add to get (23).

Theorem 3.6.

$$\frac{{}_2\phi_1(a, b; c; xq)}{{}_2\phi_1(a, b; c; x)} = \frac{h(a, b, c, xq)(1 - x)}{h(a, b, c, x)} = \frac{1 - x}{1 - bx + \dfrac{P_1}{Q_1 + \cdots}}$$

where

$$P_n = x(a - cq^{n-1})(bq^{n-1} - 1), \quad n = 1, 2, \ldots,$$

$$Q_n = 1 + ax - q^{n-1}(bxq + c), \quad n = 1, 2, \ldots.$$

Proof. Changing b to (b/q), c to (c/q) and x to xq (22) can be re

$$\frac{h(a, b, c, xq)}{h(a, b, c, x)} = \frac{1}{(1 - bx) + \dfrac{x(a - c)(b - 1)}{\dfrac{h(a, b, c, xq)}{h(a, bq, cq, xq)}}}.$$

Changing b to bq^{n-1}, c to cq^{n-1}, (23) can be rewritten as

Proof. Interchanging a and b in III′ and then ap
denominator of the left side of the resulting id

Theorem 3.8. *Let the continued fractions in the*
be denoted by $C_1(a,b,c,x)$, $C_2(a,b,c,x)$, $C_3(a$
respectively. Then,

$$\frac{{}_2\phi_1(a,b;cq,x)}{{}_2\phi_1(a,b;c;x)} = \frac{h(a,b,cq,x)(1-c)}{h(a,b,c,x)}$$
$$= \frac{1-c}{1-c\,C_i(a,b,cq,x)},$$

Proof. Identity (7) can be written as

$$\frac{h(a,b,cq,x)}{h(a,b,c,x)} = \frac{1}{1+} \frac{-c}{h(a,b,cq,x)}$$
$$(1-x)h(a,b,cq,x$$

Changing c to cq in I, II, III, IV and IV′ and using
result.

Theorem 3.9.

$$\frac{{}_2\phi_1(a,b;cq;xq)}{{}_2\phi_1(a,b;c;x)} = \frac{h(a,b,cq,xq)(1-c}{h(a,b,c,x)}$$
$$= \frac{(1-c)(1-x)}{F_1'+} \quad \frac{E}{F_2'}$$

where E_n' *and* F_n' *are obtained from* E_n *and* F_n *c*

Proof. Change x to x/q in (20) and iterate the
take the reciprocal.

Proof. Identity (12) can be written as

$$\frac{h\left(aq, b, c, \frac{x}{q}\right)}{h(a, b, c, x)} = \frac{1}{1 + \dfrac{\dfrac{x}{q}(b-c)}{\dfrac{h\left(aq, b, c, \frac{x}{q}\right)}{h(aq, b, cq, x)}}}.$$

Change a to aq and x to x/q^2 in (20), iterate the resulting equation use (26) to get XII.

Theorem 3.11.

$$\frac{{}_2\phi_1\left(a, bq; c; \frac{x}{q}\right)}{{}_2\phi_1(a, b; c; x)} = \frac{h\left(a, bq, c, \frac{x}{q}\right)}{\left(1 - \frac{x}{q}\right)h(a, b, c, x)}$$

$$= \frac{1}{1 - \frac{x}{q} + \dfrac{\frac{x}{q}(a-c)\left(1 - \frac{x}{q}\right)}{\widetilde{F}_1 + \dfrac{\widetilde{E}_2}{\widetilde{F}_2 + \cdots}}}$$

where the $\widetilde{E}_n$ and $\widetilde{F}_n$ are obtained from E_n'' and F_n'' of XII *by inte*

Proof. Interchange a and b in XII and use (3).

Theorem 3.12 is the q-analogue of Entry 20 of Chapter 12 of notebook [13], [4]. It is also the same as the following well kno fraction [9]. We only indicate here in Lemma 3.7 how the requir follow from (9) and (12).

This on using (12) and the symmetry relation (3)

$$h\left(a, bq, c, \frac{x}{q}\right) - \left(1 - \frac{x}{q}\right) h(a, b, c, x) = \frac{x}{q}$$

Changing b to b/q and x to xq and using the symm
equivalent to (9).

Theorem 3.12.

$$\frac{{}_2\phi_1(a, bq; cq; x)}{{}_2\phi_1(a, b; c; x)} = \frac{h(a, bq, cq, x)(1-c)}{h(a, b, c, x)}$$

$$= \frac{(1-c)}{(1-c)+} \frac{J_0}{(1-cq)+}$$

$$\cdots \frac{J_n}{(1-cq^{2n+1})+} \frac{}{(1}$$

where

$$J_n = x(cq^n - b)(1 - aq^n)q^n, \quad n = 0, 1, 2$$

and

$$R_n = x(cq^{n+1} - a)(1 - bq^{n+1})q^n, \quad n =$$

Theorem 3.13.

$$\frac{{}_2\phi_1(aq, b; cq; x)}{{}_2\phi_1(a, b; c; x)} = \frac{h(aq, b, cq, x)(1-c)}{h(a, b, c, x)}$$

$$= \frac{(1-c)}{(1-c)+} \frac{qR_{-1}}{(1-cq)+}$$

$$\frac{qR_{n-1}}{}$$

$$= \frac{1}{1+} \frac{aq+\lambda q}{1+} \frac{bq+\lambda q^2}{1+\cdots}$$

$$= \frac{1}{1+} \frac{aq+\lambda q}{1-aq+bq+} \frac{aq+\lambda q^2}{1-aq+bq^2+\cdots}$$

$$= \frac{1}{1-b+aq+} \frac{b+\lambda q}{1-b+aq^2+} \frac{b+\lambda q^2}{1-b+aq^3+\cdots}$$

$$= \frac{1}{1+aq+} \frac{\lambda q-abq^2}{1+aq^2+bq+} \frac{\lambda q^2-abq^4}{1+aq^3+bq^2+\cdots}.$$

Suffix R in I'_R and IV'_R signifies that the identities are due to Ramanu
signifies that the identity is due to Hirschhorn [10].

On making the substitutions (5) in V to XII and XIV and lett
respectively

$$\frac{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda q/a)_n a^n}{(q)_n(-bq)_n}}{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq)_n}} = \frac{1-\frac{ab}{\lambda}}{(1-b)-\frac{a}{\lambda q}(\lambda q+bq+b)+}$$

$$\frac{\frac{1}{\lambda^2 q}(\lambda q+a)(\lambda q+b)(\lambda q-ab)}{q(1-b)-\frac{a}{\lambda q}(\lambda q^2+bq+b)+\cdots} \frac{\frac{1}{\lambda^2 q}(\lambda q^n+a)(\lambda q^n+b)}{q^n(1-b)-\frac{a}{\lambda q}(\lambda q^{n+1}+}$$

$$\frac{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq^2)_n}}{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq)_n}}$$

$$\frac{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n(aq)^n}{(q)_n(-bq^2)_n}}{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq)_n}} = \frac{1+bq}{1+aq+bq+1-}$$

$$\cdots \frac{\lambda q^{n-1} - abq^{}}{1+aq^n+bq^n}$$

$$\frac{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda q/a)_n(a/q)^n}{(q)_n(-bq)_n}}{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq)_n}} = \frac{1}{1+} \frac{-a}{1+a+bq}$$

$$\cdots \frac{\lambda q^{n-1} -}{1+aq^{n-1}}$$

$$\frac{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n(aq)^n}{(q)_n(-bq^2)_n}}{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq)_n}} = \frac{1+bq}{1+bq+} \frac{aq+}{1+bq}$$

$$\cdots \frac{aq^{n+1} + \lambda q^{2n}}{1+bq^{2n+2}}$$

$$\frac{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(n+1)]}(-\lambda q/a)_n a^n}{(q)_n(-bq^2)_n}}{\sum_{n=0}^{\infty} \frac{q^{\frac{1}{2}[n(+1)]}(-\lambda/a)_n a^n}{(q)_n(-bq)_n}} = \frac{1+bq}{1+bq+} \frac{\lambda q - al}{1+bq}$$

$$\cdots \frac{\lambda q^{2n+1} - abq}{1+bq^{2n+2}}$$

In [8] Frank has obtained expansions of the type

$$1+\frac{xd_1}{xf_1+1+\cdots}\ \frac{xd_n}{xf_n+1+\cdots}$$

(or its reciprocal) for the ratios, mainly, of each of ${}_2\phi_1(a,bq$ ${}_2\phi_1(a,b;cq;x)$, ${}_2\phi_1(aq,bq;cq;x)$, ${}_2\phi_1(aq,bq;cq;x/q)$, ${}_2\phi_1(a,b;c;$ The functional relations needed for obtaining these expansion

$$h(a,b,c,x)-h(aq,b,c,x)=ax(b-1)h(aq,bq,cq,x)$$

$$h(a,b,c,x)-(1-c)h(a,bq,cq,x)=x(c-b)(1-a)h(aq$$

$$h(a,bq,c,x)-h(aq,b,c,x)=x(b-a)h(aq,bq,cq,x)$$

and

$$h(a,b,c,x)-(1-c)h(a,b,cq,x)=cx(1-a)(1-b)h(aq$$

The first of these is the same as (6). The other three can be shown In fact the second relation is the same as (27).

References

[1] Adiga C, Berndt B C, Bhargava S and Watson G N, Chapter 16 of Ran Theta-functions and *q*-series, *Mem. Am. Math. Soc.* **315** (1985) 1–85

[2] Andrews G E, An introduction to Ramanujan's 'lost' notebook, *Am. M*

[3] Andrews G E, Ramanujan's 'lost' notebook III. The Rogers–Ramanuj *Math.* **41** (1981) 186–208

[4] Berndt B C, Lamphere R L and Wilson B M, Chapter 12 of Ramanujan's s fractions, *Rocky Mountain J. Math.* **15** (1985) 235–310

[5] Bhargava S and Adiga C, On some continued fraction identities of Srini *Math. Soc.* **92** (1984) 13–18

[6] Bhargava S and Adiga C, Two generalizations of Ramanujan's continue *notes in mathematics* (Berlin-Heidelberg: Springer-Verlag) 1122 (1985) 5

[7] Danis R Y, On basic hypergeometric functions and continued fractions

[8] Frank E, A new class of continued fraction expansions for the ratios of

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987,
© Printed in India.

On the set of discrete subgroups of bounded covo in a semisimple group

A BOREL
School of Mathematics, The Institute for Advanced Study, I

Abstract. In this note G is a locally compact group whic groups $\mathscr{G}_s(k_s)(s\in S)$, where k_s is a local field of characteristic simple k_s-group, of k_s-rank $\geqslant 1$. We assume that the sum of t on G. Then, given a constant $c > 0$, it is shown that, up to c many irreducible discrete subgroups L of covolume $\leqslant c$ (4 H C Wang for real groups. His argument extends to the pre finitely presented (2.4) and locally rigid (3.2).

Keywords. Discrete subgroups; bounded covolume; semisi

1. Introduction

Let first G be a connected semisimple Lie group with fin factors, of $\mathbb{R}$-rank $\geqslant 2$. Fix a Haar measure on G, hence discrete subgroup. The total measure $v(G/L)$ of G/L is called be denoted $c(L)$. By a result of H C Wang [15], given a co conjugacy classes of irreducible discrete subgroups for whic Serre and Tits asked whether this is true in the p-adic case. I indeed the case. In fact, we prove more generally a sin subgroups of products of semisimple groups over local f without compact factors.

This paper answers only the first of several questior pertaining to the finiteness of the number of pairs G, L with I given constant, for a suitable a priori universal normaliz when G or even the groundfield are allowed to vary. A

compact topological group, using the topology of k_s, and let G
For $T \subset S$, let pr_T be the projection of G onto $G_T = \prod_{s \in T} G$

Let S_∞ (resp. S_f) be the set of s for which k_s is archimedean
$G_\infty = G_{s_\infty}$, $G_f = G_{S_f}$ and pr_∞ (resp. pr_f) be pr_T for $T = S_\infty$ (

Let V be the set of places of $\mathbb{Q}$. It is the union of the set of
place ∞. For $v \in V$, let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ at v. We den
which k_s contains $\mathbb{Q}_v$. We also write pr_v for pr_T when $T =$

$$R\mathscr{G}_T = \prod_{s \in T} R_{k_s/\mathbb{Q}_v} \mathscr{G}_S R G_T = \prod_{s \in T} R_{k_s/\mathbb{Q}_v} \mathscr{G}_s(\mathbb{Q}_v), \quad (T \subset$$

where $R_{k_s/\mathbb{Q}_v}$ refers to Weil's restriction of scalars [16:I]. The
$\mathbb{Q}_v$-group, and $RG_T = R\mathscr{G}_T(\mathbb{Q}_v)$ is in a natural way an ana
[16:1·3·2], there is a canonical isomorphism of topological

$$G_T = RG_T.$$

We let r_s denote the k_s-rank of $\mathscr{G}_s$ and $r(G)$ the sum of th
$r_s \geqslant 1$ for all s.

2.2. A discrete subgroup L of G is "irreducible" if there is n
non-empty subsets such that $(L \cap G_A)(L \cap G_B)$ is of finite in

2.3. *Lemma*

Let L be an irreducible subgroup of finite covolume of G.

(a) *For every $s \in S$, $\mathrm{pr}_s L$ is Zariski dense in $\mathscr{G}_s$.*
(b) *Let $T \subset S_v$. Then $\mathrm{pr}_T L$ is Zariski dense in $R\mathscr{G}_T$. Assume T
closure H of $\mathrm{pr}_T L$ contains the product of the groups G_s^+
open of finite index.*

[G_s^+ denotes the subgroup of G_s generated by the k_s-ration
unipotent k_s-subgroups of $\mathscr{G}_s$, cf. [3:§6].]

(a) follows from [9:1.12].
(b) The group $\mathrm{pr}_T L$ has the property (S) (cf. [1], [12:5.1]).

2.4. PROPOSITION

Let L be a discrete subgroup of finite covolume of G. Then L is finit

If a subgroup of finite index of L is finitely presented, then presented, as is well-known. Therefore we may assume L to be in

If $S = S_\infty$, the result is known: If one group G_s has $\mathbb{R}$-rank one, thi not, then L is arithmetic [8], in which case this is proved e.g. in [2]. L X_f the product of the Bruhat-Tits buildings of the groups G_s for operates on S_f. We claim that X_f is a finite polyhedron mod L. In fa which case L is discrete and cocompact, or $S \neq S_f$ and then $\mathrm{pr}_f L$ i subgroup of finite index (2.3). In both cases our assertion is clear. The in G_f of a face σ of X_f is a compact open subgroup. The isotropy $L \cap (G_\infty \times K_\sigma)$. Its projection on G_∞ is discrete of finite covolume. finitely presented. Then L is finitely presented by Theorem 4 in [6

Our next remark is a trivial extension to our situation of a re Margulis.

2.5. PROPOSITION

(a) *Let $S = S_f$. Then G has a compact open neighbourhood of 1 which subgroup at the identity only.*

(b) *The group G has a neighbourhood of the identity U such that if L i a conjugate of L meets U only at 1. In particular $c(L)$ has a strictl*

In case (a) we just have to take for U a torsion-free compact ope always exists.

If $G = G_\infty$, then our assertion is a well-known result of Kazh 12:XI]. Let U_∞ be such a neighbourhood in G_∞ and U_f a torsion- subgroup of G_f. Then $U = U_\infty \times U_f$ satisfies our condition.

2.6. *Lemma*

Let k be a local field, $\mathcal{H}$ an almost absolutely simple k-group, (

(u_j). This is easy: Let

$$h \cdot u_j = \sum h_{ji} u_i, \quad (h \in L).$$

Multiplying on the right by t_i and taking traces, we get

$$h_{ji} = \operatorname{tr}(h \cdot u_j \cdot t_i) = \sum_a d_{aj} \operatorname{tr}(h \cdot t_a \cdot t_j).$$

Hence $|h_{ji}|$ has a universal bound in view of our assumptions.

Note. This argument just copies a known one of E B Vinberg.

3. Local rigidity

3.1. We fix an irreducible discrete subgroup L of finite covolume of G. Let $\mathbf{a} = (a_1, \ldots, a_m)$ be a generating set for L and $w_k (k \in K)$ be a finite set of defining relations for L (2.4). As usual, the set $R(L, G)$ of homomorphisms of L into G is identified with the set of m-tuples $\mathbf{g} = (g_1, \ldots, g_m) \in G^m$ which satisfy the relations $w_k(g_1, \ldots, g_m) = 0 (k \in K)$. It is a closed subset of G^m, invariant under the group Aut G of automorphisms of G, acting componentwise in particular under the group Int G of inner automorphisms, where $x \in G$ acts by $\mathbf{g} \mapsto (xg_1x^{-1}, \ldots, xg_mx^{-1})$. The group L is said to be *locally rigid* if Int $G(\mathbf{a})$ contains a neighbourhood of $\mathbf{a}$ in $R(L, G)$.

3.2 Theorem. *Let L be as in 3.1 and assume that $r(G) \geqslant 2$. Then L is locally rigid.*

For $\mathbf{y} = (y_i) \in R(L, G)$, the map $a_i \mapsto y_i (i = 1, \ldots, m)$ extends to a homomorphism $\alpha_{\mathbf{y}}$ of L onto the subgroup $L_{\mathbf{y}}$ generated by the components y_i of $\mathbf{y}$.

(a) Let $s \in S$. We claim first that for $\mathbf{y} \in R(L, G)$ sufficiently close to $\mathbf{a}$, the group $\operatorname{pr}_s L_{\mathbf{y}}$ is Zariski-dense in $\mathscr{G}_s$ and not relatively compact in G_s.

Assume the first assertion to be false. There exists then a sequence $\mathbf{y}_i \to \mathbf{a}$ in $R(L, G)$ and, for each i, a proper subalgebra $\mathfrak{q}_i$ of the Lie algebra $\mathfrak{g}_s$ of $\mathscr{G}_s$ such that

$$\operatorname{Ad} y_{ij}(\mathfrak{q}_i) = \mathfrak{q}_i \quad (j = 1, \ldots, m).$$

Passing to a subsequence, we may assume the $\mathfrak{q}_i$ to have a constant dimension, say d, and then, again going over to a subsequence, we may assume that the $\mathfrak{q}_i(k_s)$ converge to a subspace $\mathfrak{q}$ in the Grassmannian of d-planes in $\mathfrak{g}_s(k_s)$. By continuity, Ad a_j leaves $\mathfrak{q}$ invariant for all j's, hence also for all $x \in L$, and, by (2.3) for all $x \in G_s$. But $\mathfrak{g}_s(k_s)$ is simple, whence a contradiction.

Write L_i for $L_{\mathbf{y}}$ when $\mathbf{y} = \mathbf{y}_i$. If now the $\operatorname{pr}_s L_i$ were all relatively compact, the traces of the elements of these groups in some linear realization of $\mathscr{G}_s$ would be uniformly bounded and so would be those of the elements of $\operatorname{pr}_s L$. By 2.6, $\operatorname{pr}_s L$ would be relatively compact. This however, would contradict the fact that G_s is not compact and $\operatorname{pr}_s L$ is dense in an open subgroup of G_s if $S \neq \{s\}$ (2·3), or has finite covolume if $S = \{s\}$.

(b) Let $v \in V$ and $T \subset S_v$. We assert now that for $\mathbf{y} \in R(L, G)$ sufficiently close to $\mathbf{a}$, the group $\operatorname{pr}_T L_{\mathbf{y}}$ is Zariski dense in $\mathscr{G}_T$.

If T consists of one place, this is (a). Assume then that T has at least two elements.

Let $\mathscr{M}_y$ be the Zariski closure of $\mathrm{pr}_T L_y$ and $\mathfrak{m}_y$ the Lie algebra of RM_y. In view of (a), it maps on to the Lie algebra of RG_t for any $t \in T$. Therefore, for any $x \in L_y$ the characteristic polynomial $C(\lambda, \mathrm{Ad}\,\mathrm{pr}_t(x) | L(RG_t))$ divides the characteristic polynomial $C(\lambda, \mathrm{Ad}\,\mathrm{pr}_T(x) | \mathscr{M}_y)$.

Assume (b) to be false. The previous argument, carried out in RG_T, shows the existence of a sequence $\mathbf{y}_i \in R(L, G)$ tending to $\mathbf{a}$, such that the $\mathfrak{m}_{\mathbf{y}_i}$ have a constant dimension and tend to a proper subspace $\mathfrak{q}$ of the Lie algebra $L(RG_T)$ of RG_T. For every $x \in L$, the elements $\alpha_{\mathbf{y}_i}(x)$ tend to x. Since $\mathrm{pr}_T L$ is Zariski-dense in $\mathscr{G}_T$ (2.3), it follows that $\mathfrak{q}$ is an ideal of $L(RG_T)$, proper by our assumption. It is therefore equal to the Lie algebra of $RG_{T'}$, for some $T' \subset T$, with $T' \neq \phi, T$. Fix $t \in T$. We have seen that $C(\lambda, \mathrm{pr}_t(\alpha_{\mathbf{y}_i}(x)) | L(RG_t))$ divides $C(\lambda, \mathrm{pr}_T(\alpha_{\mathbf{y}_i}(x)) | \mathscr{M}_{\mathbf{y}_i}))$. By continuity, it follows that for all $x \in L$, $C(\lambda, \mathrm{Ad}\,\mathrm{pr}_t(x) | L(RG_t))$ divides $C(\lambda, \mathrm{Ad}\,\mathrm{pr}_T(x) | L(G_{T'}))$. By Zariski-density, this should then be true for any $x \in G_T$. But, for $t \in T$, $t \notin T'$, this is absurd. This contradiction proves (b).

(c) Let $v \in V$ be finite and $T \subset S_v$. We now claim that for $\mathbf{y} \in R(L, G)$ sufficiently close to $\mathbf{a}$, the group $\mathrm{pr}_T L_y$ contains an open subgroup of finite index of RG_T.

We know that $\mathrm{pr}_T L$ is dense in an open subgroup of finite index of RG_T (2.3). We claim that $\mathrm{pr}_T L_y$ is not discrete if $\mathbf{y}$ is close enough to $\mathbf{a}$. If it were discrete, then there would be a sequence $\mathbf{y}_i \to \mathbf{a}$, such that the closure of the union of the $L_{\mathbf{y}_i}$ would contain $\mathrm{pr}_T L$, hence, by (2.3), an open subgroup of finite index of RG_T, but this contradicts 2.5(a). Combined with (b), this shows that $\mathrm{pr}_T L_y$ is dense in an open subgroup H of RG_T for $\mathbf{y}$ close to $\mathbf{a}$. Let $t \in T$ and $T' = T - \{t\}$. The kernel N of the restriction of $\mathrm{pr}_{T'}$ to H is then open in G_t. Since G_t^+ is simple modulo center [12], it follows that $G_t^+ \subset N$. Therefore, H contains the product of the G_t^+ ($t \in T$). Since G_t^+ has finite index in G_t, our assertion follows.

(d) We assume here that all $\mathscr{G}_s$ are of adjoint type, hence absolutely simple. We fix $\mathbf{y} \in R(L, G)$ close enough to $\mathbf{a}$ so that (b) and (c) hold for L_y. We write L' and α for L_y and α_y. We want to prove that α extends to an automorphism of G.

Fix s. By [8], there exist $t = t(s) \in S$, a continuous homomorphism $\mu_s : k_t \to k_s$ and a k_s-morphism $\nu_s : {}^{\mu_s}\mathscr{G}_t \to \mathscr{G}_s$ such that the composition

$$\sigma_s : G \xrightarrow{\mathrm{pr}_t} G_t \xrightarrow{\mu_s^0} {}^{\mu_s}\mathscr{G}_t(\mu_s(k_t)) \xrightarrow{j} {}^{\mu_s}\mathscr{G}_t(k_s) \xrightarrow{\nu_s(k_s)} G_s \tag{3}$$

extends $\mathrm{pr}_s \circ \alpha : L \to \mathrm{pr}_s L'$.

We claim that in fact μ_s is an isomorphism. The morphism ν_s is non-trivial, hence is a k_s-isomorphism, since both groups are absolutely k_s-simple. Therefore $\nu_s(k_s)$ is an isomorphism of topological groups. The third arrow in (3) is just induced by the inclusion $\mu_s(k_t) \to k_s$. If it were not surjective, then $\mathrm{Im}\, j$ would be a closed subgroup H if infinite index, not discrete, not relatively compact and $\mathrm{pr}_s L'$ would be contained in such a subgroup. The Lie algebra of H in $L(RG_s)$ would be proper, contradicting the Zariski density of $\mathrm{pr}_s(L')$. Therefore, σ_s is a continuous and open surjective homomorphism of G onto G_s, which extends $\mathrm{pr}_s \circ \alpha$, and whose kernel is the product of the factors G_u with $u \neq t$. Let now σ be the product of the σ_s. It is a continuous homomorphism of G into G which extends α. We want to prove that σ is an automorphism.

Now that j is the identity in k_s we see that $\nu_s(k_s) \circ \mu_s^0$ is an isomorphism of $G_{t(s)}$ onto G_s. It suffices therefore to show that $s \mapsto t(s)$ is a permutation of S, or, equivalently, that no G_s is contained in the kernel of σ.

Of course, $s \mapsto t(s)$ leaves each S_v stable. It is therefore equivalent to show that σ induces an automorphism of G_{S_v} onto itself for every $v \in V$, and for this that no G_s belongs to the kernel of $\sigma | G_v$. Assume to the contrary that $\sigma(G_s) = 1$ for some $s \in S_v$. Then Card $S_v \geqslant 2$. Let $T' = S_v - \{s\}$ and $T = S_v$. The homomorphism σ induces a continuous homomorphism of G_T, into G_T hence also of RG_T, into RG_T. These groups are analytic over $\mathbb{Q}_v$, hence σ is analytic [5:III, § 8]. The image is then a proper Lie subgroup H, whose projection on each factor RG_s is equal to $RG_s (s \in T')$. Its Lie algebra $\mathfrak{h}$ maps onto the Lie algebra of RG_s under $\mathrm{pr}_s (s \in T')$. On the other hand, $\mathfrak{h}$ should be invariant under $\mathrm{pr}_{T'} L$, hence under Zariski dense subgroup (see (b)), and should therefore be a proper ideal. But this contradicts the previous surjectivity assertion.

(e) The automorphism σ belongs to the group $A(G)$ of automorphisms of G which are compositions of permutations of factors, field isomorphisms and restrictions to rational points of morphisms of algebraic groups of the various factors. [These are in fact all automorphisms of G, but we need not know that.] In this group the product B of the groups $\mathrm{Aut}\, \mathscr{G}_s(k_s)$ is open of finite index. Therefore $\mathrm{Int}\, G = \Pi_{s \in S} \mathrm{Int}\, G_s$ is also open of finite index in $A(G)$.

(f) We can now prove the theorem. Let $\mathscr{G}'_s = \mathrm{Ad}\, \mathscr{G}_s$ and let $\pi_s : \mathscr{G}_s \to \mathscr{G}'_s$ be the canonical isogeny ($s \in S$). The morphism $\pi_s(k_s) : G_s \to G'_s$ has finite kernel, hence is proper, and its image is open of finite index [3:3.19], therefore the same is true for the product $\pi : G \to G'$ of the $\pi_s(k_s)$. In view of (e), $\pi(G)$ is also open of finite index in $A(G')$. In fact, π is a local homeomorphism.

Since π is proper and with image open of finite index, $L' = \pi(L)$ is discrete, of finite covolume in G'. With the notation and conventions of 3.1, let $\mathbf{a}' \in R(L', G')$ be the point with components $\mathbf{a}'_i = \pi(a_i)$ $(i = 1, \ldots, m)$ in G'^m. By (d), $A(G')(\mathbf{a}')$ contains a neighbourhood of $\mathbf{a}'$ in $R(L, G')$. By homogeneity, $A(G')(\mathbf{a}')$ is open in $R(L', G')$. Since all spaces under consideration are locally compact, countable at infinity, the orbit map $\beta : x \mapsto x \cdot \mathbf{a}'$ induces a homeomorphism of $A(G')/H$, where H is the isotropy group of $\mathbf{a}'$, onto $A(G')(\mathbf{a}')$ [4:VII, App. 1]. In particular, for every neighbourhood U of 1 in $A(G')$, $\beta(U)$ is a neighbourhood of $\mathbf{a}'$ in $R(L', G')$.

The group $\pi(G)$, identified to a subgroup of $A(G')$ via the inclusion of $G' = \mathrm{Int}\, G'$ into $A(G')$, is also open of finite index. If we let it act on $R(L', G')$ via this homomorphism, it follows that $g \mapsto g \cdot \mathbf{a}'$ is an open map.

Fix now an open neighbourhood V of $\mathbf{a}$ in G^m which is mapped homeomorphically onto a neighbourhood V' of $\mathbf{a}'$ by π. Let U be a neighbourhood of 1 in G such that $\mathrm{Int}\, g \cdot \mathbf{a} \subset V$ for $g \in U$. If now $\mathbf{y} \in R(L, G)$ is such that $\pi(\mathbf{y}) \in U \cdot \mathbf{a}'$, then there exists $g \in U$ such that $g \cdot \mathbf{a} = \pi(\mathbf{y})$. It follows that $g \cdot \mathbf{a}$ is an element of V which maps onto $\pi(\mathbf{y})$, hence $g \cdot \mathbf{a} = \mathbf{y}$. Therefore L is locally rigid.

4. Covolumes

4.1. The group G is locally compact, therefore the space of closed subgroups of G, endowed with the topology defined in [4:VIII, § 5] is compact. For any neighbourhood U of the identity, the subspace N_U of discrete subgroups which meet U only at 1 form a compact subset [4:VIII, § 5, no. 3, Prop. 7]. Moreover, the function $L \mapsto c(L)$ is lower semi-continuous [4:VIII, § 5, no. 2, Prop. 4]. In particular if a sequence of elements L_i of N_U tends to L and $c(L_i) \leqslant c$ for all i, then $c(L) \leqslant c$. We recall that $L_i \mapsto L$ if and only if

the following condition is fulfilled (*loc. cit.*, no. 6): For any compact set $C \subset G$ and any neighbourhood U of 1 in G, we have

$$L_i \cap C \subset L \cdot U \text{ and } L \cap C \subset L_i \cdot U \text{ for } i \text{ big enough.} \tag{4}$$

4.2 Theorem. *Fix a constant $c > 0$. Assume $r(G) \geqslant 2$. Then the discrete subgroups of G with covolume $c(L) \leqslant c$ form finitely many conjugacy classes.*

In view of 2.3, 2.4, 3.2 and 4.1, the argument of H C Wang in the real case [15] goes over without change. For the sake of completeness, we describe it briefly.

Assume 4.2 to be false. Then we can find an infinite sequence L_i of nonconjugate discrete subgroups with covolume $\leqslant c$. Passing to a subsequence, we may assume that $c(L_i)$ has a limit $b \leqslant c$. Replacing L_i by a conjugate, if necessary, we may assume that $L_i \cap U = 1$, where U is a suitable neighbourhood of 1 in G (2.5). Then a cofinal subsequence of the L_i's has a limit L and $c(L) \leqslant b$ (4.1). We now consider the setup of 3.1. Let $a_1, \ldots, a_m$ be a generating set for L and w_k ($k \in K$) a finite defining set of relations (2.4). By 4.1, we can find $x_{ij} \in L_i$ such that

$$\lim_{i \to \infty} x_{ij} = a_j \quad (j = 1, \ldots, m).$$

For i big enough, we have then $w_k(x_{i1}, \ldots, x_{im}) \in U \cap L_i$, hence $w_k(x_{i1}, \ldots, x_{im}) = 1$ ($k \in K$). Therefore the map $a_j \mapsto x_{ij}$ ($j = 1, \ldots, m$) extends to a homomorphism of L onto the subgroup L_i' of L_i generated by the x_{ij}'s, and $x_i = (x_{i1}, \ldots, x_{im})$ is a point of $R(L, G)$, which comes arbitrarily close to $\mathbf{a}$ if i is big enough. For such i's, L_i' is by 3.2 conjugate to L under an inner automorphism. In particular $c(L_i') = c(L)$, and L_i' has finite index in L_i. Then $c(L_i')/c(L_i)$ is an integer $\geqslant 1$. On the other hand, it is equal to $c(L)/c(L_i)$, hence tends to $c(L)/b$, which is $\leqslant 1$. Altogether we get $c(L_i') = c(L_i) = c(L)$, hence $L_i = L_i'$ and L_i is conjugate to L The L_i's are therefore pairwise conjugate for i big enough, whence a contradiction.

Remarks

(1) In the real case, the result of [15] is also valid if $r(G) = 1$, provided that G is not locally isomorphic to $SL_2(\mathbb{R})$ or $SL_2(\mathbb{C})$. [In fact, H C Wang ruled only $SL_2(\mathbb{R})$ out, but this was an oversight.] In the p-adic case, this is however false, since a torsion-free discrete subgroup of finite covolume of a simple p-adic group of relative rank one is cocompact and free.

(2) The previous argument also proves the following statement: Let L be a discrete finitely generated subgroup of G which is locally rigid, and $\{L_i\}$ a sequence of discrete subgroups of G which tend to L. If the L_i's are cocompact, then L is also cocompact.

In fact, the above proof shows that L is conjugate to a subgroup of L_i for i big enough.

Of the real groups G under consideration here, without restriction on the $\mathbb{R}$-rank, only groups locally isomorphic to $SL_2(\mathbb{R})$ or $SL_2(\mathbb{C})$ have discrete subgroups of finite covolume which are not locally rigid. On the other hand, they do contain sequences of discrete cocompact subgroups converging to a discrete non-cocompact subgroup of finite covolume: for $SL_2(\mathbb{C})$, such sequences are obtained by Dehn surgery. In $SL_2(\mathbb{R})$, such examples are easy to obtain geometrically: For instance we may consider a

We set $k' := \sqrt{(1-k^2)}$, $K'(k) := K(\sqrt{(1-k^2)})$, $E'(k) := E(\sqrt{(1-k^2)})$. We then have the key relations

$$K(k) = \frac{\pi}{2}\theta_3^2(q), \quad k := k(q) = \frac{\theta_2^2(q)}{\theta_3^2(q)} \quad \text{and} \quad q := \exp(-\pi K'/K), \tag{1}$$

where the *special theta functions* are given by

$$\theta_3(q) := \sum_{n=-\infty}^{\infty} q^{n^2} \quad \text{and} \quad \theta_2(q) := \sum_{n=-\infty}^{\infty} q^{(n+1/2)^2}.$$

The *singular value function* is then defined by

$$k(N) := k[\exp(-\pi\sqrt{N})] \quad \text{or} \quad K'(k(N))/K(k(N)) = \sqrt{N} \tag{2}$$

for positive N. This uniquely defines k on $(0, \infty)$ as a decreasing function with $k(0) = \infty$, $k(1) = 1/\sqrt{2}$, and $k(\infty) = 0$. Also k is algebraic when N is rational [2]. In [2] a corresponding function α (*a singular value of the second kind*) was studied. It is defined by

$$\alpha(N) := (E'/K) - (\pi/4K^2) \qquad k := k(N) \cdot \tag{3}$$

and likewise is algebraic at rational values with $\alpha(1) = 1/2$, $\alpha(\infty) = 1/\pi$. Moreover, α satisfies recursions which allow for its computation both algebraically and numerically. For example,

$$\alpha(4N) = (1 + k(4N))^2\alpha(N) - 2\sqrt{N}k(4N) \tag{4}$$

and

$$k(4N) = [1 - k'(N)]/[1 + k'(N)]. \tag{5}$$

This type of relation can then be iterated and leads to high-order iterations for π (see [2], [3] and below). The function alpha is directly connected to *Ramanujan's multiplier* R_N which is defined in terms of the Eisenstein series

$$P(q) := 1 - 24\sum_{n=1}^{\infty} \frac{nq^{2n}}{1-q^{2n}} \tag{6}$$

by

$$R_N(l, k) := \frac{NP(q^N) - P(q)}{\theta_3^2(q)\theta_3^2(q^N)} \quad k = k(q^N) \quad l = k(q). \tag{7}$$

Ramanujan gives closed forms for R_N for $N = 2, 3, 5, 7, 11, 15, 17, 19, 23, 31$ and 35, many of which we use below (see [2] and [6]). From now on we will freely write k and l for

$$k = k(N^2r) = k[\exp(-\pi N\sqrt{r})], \quad l = k(r) = k[\exp(-\pi\sqrt{r})].$$

The pair of modulii k and l then solve the *Nth order modular equation* for K and so satisfy an algebraic equation

$$W_N(l, k) = 0.$$

The corresponding *multiplier* defined by

$$M_N(l,k) := K(k)/K(l) = \theta_3^2(q^N)/\theta_3^2(q) \tag{8}$$

is then also algebraic.

We will often suppress variables and subscripts. Thus we write $m := m_N = m_N(l,k)$ where

$$m_N(l,k) := [K(l)/K(k)] - M_N^{-1}(l,k). \tag{9}$$

In these terms the recursive approximations to pi given in Chapter 5 of [2] can be described by

$$\alpha(N^2 r) = m_N^2 \alpha(r) - \sqrt{r}\varepsilon_N(r), \tag{10a}$$

where

$$\varepsilon_N(r) := \frac{m_N^2 - N}{2} + \frac{m_N}{3}\left\{ R_N + m_N(l^2 - \tfrac{1}{2}) - \frac{N}{m_N}(k^2 - \tfrac{1}{2}) \right\} \tag{10b}$$

and

$$k = k[\exp(-\pi N\sqrt{r})], \quad l = k[\exp(-\pi\sqrt{r})].$$

The accuracy of these approximations is phenomenal. For $r > 1$ the error satisfies

$$0 < \alpha(r) - 1/\pi < 16\sqrt{r}\exp(-\pi\sqrt{r}) \tag{11}$$

and this is for all intents the asymptotic if '8' replaces '16'.

An Nth order iteration for π consists of the following. Commence with $k_0 := k(r)$ and $\alpha_0 := \alpha(r)$ for some given r and then repeatedly solve $W_N(k_n, k_{n+1}) = 0$ for k_{n+1} given k_n, while using (10) with $l = k_n$, $k = k_{n+1}$ to compute $\alpha_{n+1} := \alpha(N^{2n+2}r)$. Then (11) shows that the error between α_n and $1/\pi$ is of the order of $N^n \exp[(-\pi\sqrt{r})N^n]$ and that the number of decimal digits correct increases by more than a factor of N at each step.

3. Specific examples

To compute ε_N explicitly one needs tractable forms of R_N, and of $m_N - N/m_N$. The transformation of $q \to -q$ in the latter then provides a formula for $m_N(1-l^2) - (1-k^2)N/m_N$ and the component pieces may with some effort be folded together—use of modular symmetries somewhat simplifies the task. The resulting results are surprisingly simple, especially for $N \equiv 3 \pmod 4$. We list these cumulative results next. In each case the first entry gives a form of the modular equation W_N, the second $m_N - N/m_N$, while ε_N is given third.

For $N = 3, 5, 7$ alternative solvable modular equations for m_N are given in [2] and [3]. In each case the tabular entry can be converted into a iteration for π or used to approximate log or other quantities. We also observe that the formula for ε_N can be used to determine a closed form for $dM_N(l,k)/dk$.

Explicit examples with $N \equiv 3 \pmod 4$

$N = 3$ (i) $(kl)^{1/2} + (k'l')^{1/2} = 1$,
(ii) $m - 3/m = 2[(kl)^{1/2} - (k'l')^{1/2}] = 2(kl - k'l')$,
(iii) $\varepsilon_3 = (m^2 + 2m - 3)/2$.

$N = 7$ (i) $(kl)^{1/4} + (k'l')^{1/4} = 1$,
(ii) $m - 7/m = 2[(kl)^{1/4} - (k'l')^{1/4}][2 + (kl)^{1/2} + (k'l')^{1/2}]$,
(iii) $\varepsilon_7 = (m^2 + 2m - 7)/2 + m[2(kl)^{1/2} + 2(k'l')^{1/2}]$.

$N = 11$ (i) $(kl)^{1/2} + (k'l')^{1/2} + 2(4klk'l')^{1/6} = 1$,
(ii) $m - 11/m = 2[(kl)^{1/2} - (k'l')^{1/2}][4 + (kl)^{1/2} + (k'l')^{1/2}]$,
(iii) $\varepsilon_{11} = (m^2 + 2m - 11)/2 + m[1 + (kl)^{1/2} + (k'l')^{1/2}]^2$.

$N = 15$ (i) $P^3 = 4PQ - R$ where $P = 1 + (kl)^{1/4} + (k'l')^{1/4}$
$Q = (kl)^{1/4} + (k'l')^{1/4} + (klk'l')^{1/4}$ $R = 4(klk'l')^{1/4}$,
(ii) $m - 15/m = [(kl)^{1/4} - (k'l')^{1/4}](P^3 + 2P^2 - 2P + 2)$,
(iii) $\varepsilon_{15} = (m^2 - 2m - 15)/2 + m[(kl)^{1/4} + (k'l')^{1/4}](4Q + 4)$.

$N = 23$ (i) $(kl)^{1/4} + (k'l')^{1/4} + \sqrt{2(4klk'l')^{1/12}} = 1$ $[T = (kl)^{1/4} + (k'l')^{1/4}]$,
(ii) $m - 23/m = [(kl)^{1/4} - (k'l')^{1/4}](T^4 + 3T^3 + 3T^2 + 7T + 8)$,
(iii) $\varepsilon_{23} = (m^2 + 2m - 23)/2 + m(T^5 + 3T^3 + T^2 + 4T + 1)$.

In all these cases Ramanujan has provided a formula for R_N [6] while for $N = 7, 11, 23$ he gives a form of $m_N - N/m_N$ [1]. The calculation of $m_N - N/m_N$ for $N = 3$ is straightforward, while for $N = 15$ we discovered the formula computationally. The modular equations used may be found in a variety of places. Many are derivable from or are included in the notebooks [1]. Ramanujan's formulae are usually but not always the simplest available. For example, Ramanujan gives

$$R_{23}(l, k) = 11(1 + kl + k'l') - 16(4kk'll')^{1/6}[1 + (kl)^{1/2} + (k'l')^{1/2}] - 20(4kk'll')^{1/3},$$

which we recast as

$$R_{23}(l, k) = 3(1 + kl + k'l') + 4[1 + (kl)^{1/2} + (k'l')^{1/2}]^2 - 4(4kk'll')^{1/3}$$

by using W_{23}.

For comparison we also list the following:

$N = 2$ (i) $k = (1 - l')/(1 + l')$,
(ii) $m = 1 + k = 2/(1 + l')$,
(iii) $\varepsilon_2 = 2k$.

$N = 4$ (i) $\sqrt{k} = (1 - (1 - l^2)^{1/4})/(1 + (1 - l^2)^{1/4})$,
(ii) $m = (1 + \sqrt{k})^2$,
(iii) $\varepsilon_4 = 4\sqrt{k}[1 + \sqrt{k} + k]$.

$N = 5$ (i) $k^{3/2} - l^{3/2} + 4(kl)^{1/4}(1 - kl) + 5(kl)^{1/2}(k^{1/2} - l^{1/2}) = 0$,
(ii) $m + 5/m = 2[2 + kl + k'l']$,
(iii) $\varepsilon_5 = (m^2 - 5)/2 + [m(m^2 - 2m + 5)]^{1/2}$.

We also indicate the components for $N = 19$ where Ramanujan does not provide an expression for $m_N - N/m_N$ and we have not been able to determine a suitable formula, although R_{19} is simple.

$N = 19$ (i) $P^5 = 7P^2R - 16QR$ where $P = (kl)^{1/2} + (k'l')^{1/2} - 1$
$Q = (klk'l')^{1/2} - (kl)^{1/2} - (k'l')^{1/2}$ $R = -16(klk'l')^{1/2}$,
(ii) $R_{19} = 6[(1 + kl + k'l') + (kl)^{1/2} + (k'l')^{1/2} - (klk'l')^{1/2}] = 6P^2 - 18Q$
$m_{19} = \{1 + [(A - B - 1)^{1/2} - (AB)^{1/2}]^2\}[(1 + kl + k'l')/2]^{-1/2}$
$A = k'^{3/4}l'^{-1/4}$ $B = k^{3/4}l^{-1/4}$.

4. Additional comments

It is worth emphasising the staggering rate of convergence of the algorithms based on these recursions. The two most natural starting values for the Nth order algorithm are $r = 1$ and $r = 1/N$. As observed, for $r = 1$ we have $k_0 = 1/\sqrt{2}$ and $\alpha_0 = 1/2$. For $r = 1/N$ one knows that k_N is the Nth singular value and solves $W_N(k'_N, k_N) = 0$ while $M_N(k'_N, k_N) = 1/\sqrt{N}$. Thus we can use (10b) or the corresponding tabular entry to obtain

$$\alpha(N) - N\alpha(1/N) = \varepsilon_N(1/N)/\sqrt{N}.$$

In addition one always has

$$\alpha(N) + N\alpha(1/N) = \sqrt{N}.$$

Thus one may determine that

$$\alpha(N) = \tfrac{1}{2}(\sqrt{N} - \varepsilon_N/\sqrt{N}) \quad \text{and} \quad \alpha(1/N) = (\sqrt{N} + \varepsilon_N/\sqrt{N})/2N,$$

where $\varepsilon_N = \varepsilon_N(1/N)$.

Example. We show how this works for various N. Throughout we let $\delta(N) := \varepsilon_N/\sqrt{N}$. Note that $1/\pi = 0{\cdot}3183099\ldots$.

($N = 3$) Setting $l = k'$ in (i) yields $2k_3k'_3 = 1/2$.
Moreover, $m_3 = \sqrt{3}$ so that, using (iii), $\varepsilon_3(1/3) = \sqrt{3}$. Thus

$$\alpha(3) = (\sqrt{3} - 1)/2 = 0{\cdot}3660\ldots.$$

($N = 7$) Setting $l = k'$ in (i) yields $2k_7k'_7 = 1/8$.
Now $m_7 = \sqrt{7}$ so that, using (iii), $\delta_7(1/7) = (1 + 4(k_7k'_7)^{1/2}) = 2$ and

$$\alpha(7) = (\sqrt{7} - 2)/2 = 0{\cdot}3228\ldots.$$

($N = 11$) Setting $l = k'$ in (i) and letting $x := 2\sqrt{(k_{11}k'_{11})}$ produces the cubic equation $(1-x)^3 = (2x)^2$. This can be solved to produce

$$2kk' = (2\gamma - 5)/6$$

with

$$\gamma := (3\sqrt{33} + 17)^{1/3} - (3\sqrt{33} - 17)^{1/3}.$$

Also, (iii) becomes $\delta(11) = 1 + (1+x)^2 = (5 + 2\gamma + 2\gamma^2)/9$ and

$$\alpha(11) = (\sqrt{11} - \delta(11))/2 = 0{\cdot}3190\ldots.$$

($N = 15$) Setting $l = k'$ in (i) leads to

$$kk' = ((\sqrt{5}-1)/4)^4 = (\sin \pi/10)^4.$$

If G denotes the golden mean, $(\sqrt{5}-1)/2$, (iii) becomes

$$\delta(15) = G(4 + 4G + G^2) - 1 = \sqrt{5} + 1 \text{ and}$$

$$\alpha(15) = (\sqrt{15} - \sqrt{5} - 1)/2 = 0{\cdot}31845\ldots.$$

($N = 23$) Setting $l = k'$ in (i) and letting $x := 2(k_{23}k'_{23})^{1/4}$ produces the cubic equation $(1-x)^3 = x^2$. This can be solved to produce

$$2kk' = \tfrac{1}{8}\gamma^{12}$$

with

$$\gamma := \frac{1}{3}\left(\left(\frac{25 + 3\sqrt{69}}{2}\right)^{1/3} + \left(\frac{25 - 3\sqrt{69}}{2}\right)^{1/3} - 1\right).$$

Also, (iii) becomes $\delta(23) = 4 + 2x^3 = 4 + 2\gamma^9$. Finally, as $\gamma^3 + \gamma^2 = 1$

$$\alpha(23) = (\sqrt{23} - 2\gamma^2 - 4\gamma)/2 = 0{\cdot}31832\ldots.$$

We conclude by presenting the asymptotics of some of these iterations commencing with the previously discussed starting values, using (11). The effect of commencing with $r = N$ instead of $r = 1/N$ is to move one index along in the iteration count. The estimate is of $\pi - 1/\alpha_n$.

	Decimal digits correct after iteration n										
n	1	2	3	4	5	6	7	8	9	10	
$r = 1$	1	3	8	19	40	84	171	345	694	1392	$N = 2$
$r = 1/2$	0	2	5	13	28	58	120	243	490	983	
$r = 1$	2	10	34	107	327	990	2979	8946	26849	80559	$N = 3$
$r = 1/3$	0	5	18	60	188	570	1718	5163	15499	46508	
$r = 1$	7	63	464	3271	22925						$N = 7$
$r = 1/7$	1	22	173	1233	8662						
$r = 1$	12	161	1811	19970	219727						$N = 11$
$r = 1/11$	2	47	543	6018	66246						
$r = 1$	28	717	16595	381801	8781586						$N = 23$
$r = 1/23$	4	147	3456	79606	1831081						

The first iteration with $r = 1/N$ produces $\alpha(N)$ as given explicitly above for 3, 7, 11, 23. The tenth iteration with $N = 11$ and $r = 1$ produces in excess of $1{\cdot}45 \cdot 10^8$ digits coincidence with $1/\pi$. The eighth iteration with $N = 23$ and $r = 1$ produces in excess of 10^{12} digits coincidence with $1/\pi$.

References

[1] Berndt B C, *Chapters 19 and 20 of Ramanujan's second notebook* (Springer Verlag) (to appear)

[2] Borwein J M and Borwein P B, *Pi and the AGM: A study in analytic number theory and computational complexity* (New York: John Wiley) (1987)

[3] Borwein J M, Borwein P B and Bailey D H, Ramanujan, modular equations and pi: or how to compute a billion digits of pi, *MAA Monthly* (in press)

[4] Hardy G H, *Ramanujan's collected papers* (New York: Chelsea Publishing) (1962)

[5] Magnus W, Formulae and theorems for the special functions of mathematical physics (Berlin: Springer Verlag) (1966)

[6] Ramanujan S, Modular equations and approximations to π, *Q. J. Math. Oxford* **45** (1914) 350–372 (New York: Chelsea) (1980)

[7] Weber H, *Lehrbuch der algebra* (Baruschweig) vol. 3 (1908)

[8] Whittaker E T and Watson G N, *Modern analysis* (Cambridge: University Press) 4th edn (1927)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 61–66.
© Printed in India.

Almost poised basic hypergeometric series

DAVID M BRESSOUD*
Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802, USA

Abstract. Given a basic hypergeometric series with numerator parameters $a_1, a_2, \ldots, a_r$ and denominator parameters $b_2, \ldots, b_r$, we say it is *almost poised* if $b_i = a_1 q^{\delta_i}/a_i$, $\delta_i = 0, 1$ or 2, for $2 \leqslant i \leqslant r$. Identities are given for almost poised series with $r = 3$ and $r = 5$ when $a_1 = q^{-2n}$.

Keywords. Hypergeometric series; poised series.

A hypergeometric series is a power series, say

$$1 + \sum a_n x^n, \quad n \geqslant 1,$$

for which the ratio of successive coefficients, a_n/a_{n-1}, is a rational function of n. A basic hypergeometric series is a power series in which the ratio of successive coefficients is a rational function in q^n. Traditionally,

$$q = \exp(2\pi i\tau),$$

where τ is a complex variable in the upper half plane. Many theta function identities are most easily understood as identities on basic hypergeometric series. Ramanujan contributed appreciably to our knowledge and understanding of these series. They permeate all of his work.

We shall restrict our attention to series of the form

$${}_r\varphi_{r-1}\left(\begin{matrix}a_1, a_2, \ldots, a_r \\ b_2, \ldots, b_r\end{matrix}; x\right) = 1 + \sum \frac{(a_1)_n (a_2)_n \cdots (a_r)_n}{(q)_n (b_2)_n \cdots (b_r)_n} x^n, \quad n \geqslant 1,$$

where

$$(a)_n = \prod \frac{(1 - aq^i)}{(1 - aq^{n+i})}, \quad i \geqslant 0,$$

$$= (1 - a)(1 - aq) \cdots (1 - aq^{n-1}).$$

Observe that the first equality defines $(a)_n$ for all real n.

Following W N Bailey [3], we call the series *well-poised* if $b_i = a_1 q/a_i$ for $2 \leqslant i \leqslant r$. F H Jackson [5] has proved the following identities for well-poised basic hyper-

* Partially supported by N.S.F. Grant No. DMS-8521580.

geometric series:

$$
{}_5\varphi_4\left(\begin{matrix}q^{-2n}, b, c, d, e\\ b^{-1}q^{1-2n}, c^{-1}q^{1-2n}, d^{-1}q^{1-2n}, e^{-1}q^{1-2n}\end{matrix}; \frac{q^{2-3n}}{bcde}\right)
$$

$$
= \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{1-2n})_n (b^{-1}d^{-1}q^{1-2n})_n (c^{-1}d^{-1}q^{1-2n})_n}{(b^{-1}q^{1-2n})_n (c^{-1}q^{1-2n})_n (d^{-1}q^{1-2n})_n (b^{-1}c^{-1}d^{-1}q^{1-2n})_n}, \tag{1}
$$

provided $bcde = q^{1-3n}$,

$$
{}_3\varphi_2\left(\begin{matrix}q^{-2n}, b, c\\ q^{1-2n}/b, q^{1-2n}/c\end{matrix}; \frac{q^{1-n}}{bc}\right) = \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{1-2n})_n}{(b^{-1}q^{1-2n})_n (c^{-1}q^{1-2n})_n}. \tag{2}
$$

Bailey [3] defined a series to be *nearly poised* if $b_i = a_1 q/a_i$ for all but one value of i in $2 \leqslant i \leqslant r$. We shall instead give identities for what we term *almost poised* series where

$$
b_i = a_1 q^{\delta_i}/a_i, \quad 2 \leqslant i \leqslant r,
$$

where δ_i is 0, 1 or 2.

$$
{}_5\varphi_4\left(\begin{matrix}q^{-2n}, b, c, d, e\\ b^{-1}q^{-2n}, c^{-1}q^{-2n}, d^{-1}q^{1-2n}, e^{-1}q^{1-2n}\end{matrix}; \frac{q^{1-3n}}{bcde}\right)
$$

$$
= \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{-2n})_n}{(b^{-1}q^{-2n})_n (c^{-1}q^{-2n})_n} {}_3\varphi_2\left(\begin{matrix}b, c, q^{-n}\\ d^{-1}q^{1-2n}, e^{-1}q^{1-2n}\end{matrix}; q\right), \tag{3}
$$

provided $bcde = q^{-3n}$,

$$
{}_3\varphi_2\left(\begin{matrix}q^{-2n}, b, c\\ b^{-1}q^{-2n}, c^{-1}q^{-2n}\end{matrix}; \frac{q^{-n}}{bc}\right) = \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{-2n})_n}{(b^{-1}q^{-2n})_n (c^{-1}q^{-2n})_n}, \tag{4}
$$

$$
{}_3\varphi_2\left(\begin{matrix}q^{-2n}, b, c\\ b^{-1}q^{-2n}, c^{-1}q^{1-2n}\end{matrix}; \frac{q^{1-n}}{bc}\right) = \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{1-2n})_n}{(b^{-1}q^{-2n})_n (c^{-1}q^{1-2n})_n}, \tag{5}
$$

$$
{}_3\varphi_2\left(\begin{matrix}q^{-2n}, b, c\\ b^{-1}q^{-2n}, c^{-1}q^{1-2n}\end{matrix}; \frac{q^{-n}}{bc}\right)
$$

$$
= \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{1-2n})_n}{(b^{-1}q^{-2n})_n (c^{-1}q^{1-2n})_n} \left\{1 - c^{-1}q^{-n} \frac{(1-q^{-n})}{(1-b^{-1}c^{-1}q^{-2n})}\right\}, \tag{6}
$$

$$
{}_3\varphi_2\left(\begin{matrix}q^{-2n}, b, c\\ b^{-1}q^{-2n}, c^{-1}q^{2-2n}\end{matrix}; \frac{q^{1-n}}{bc}\right)
$$

$$
= \frac{(q^{-2n})_n (b^{-1}c^{-1}q^{2-2n})_n}{(b^{-1}q^{-2n})_n (c^{-1}q^{2-2n})_n} \left\{1 + c^{-1}q^{-n} \frac{(1-b^{-1})}{(1-c^{-1}q)}\right\}. \tag{7}
$$

It should be kept in mind that each of these represents several identities which can be obtained from the given identity by either replacing b, c and q by b^{-1}, c^{-1} and

q^{-1}, respectively, and then using the identity

$$\prod_{i=0}^{n-1}\frac{(1-a^{-1}q^{-i})}{(1-b^{-1}q^{-i})}=\frac{(a)_n}{(b)_n}\left(\frac{b}{a}\right)^n, \tag{8}$$

or by reversing the order of summation and using the identity

$$\begin{aligned}\frac{(a)_{2n-i}}{(b)_{2n-i}}&=\frac{(a)_{2n}(bq^{2n-i})_i}{(b)_{2n}(aq^{2n-i})_i}\\&=\frac{(a)_{2n}}{(b)_{2n}}\frac{(b^{-1}q^{1-2n})_i}{(a^{-1}q^{1-2n})_i}\left(\frac{b}{a}\right)^i,\end{aligned} \tag{9}$$

or by doing both. As an example, from (4) we derive three equivalent identities

$${}_3\varphi_2\left(\begin{matrix}q^{-2n},b,c\\b^{-1}q^{-2n},c^{-1}q^{-2n}\end{matrix};\frac{q^{1-n}}{bc}\right)=\frac{(q^{-2n})_n(b^{-1}c^{-1}q^{-2n})_n}{(b^{-1}q^{-2n})_n(c^{-1}q^{-2n})_n}, \tag{10}$$

$$\begin{aligned}&{}_3\varphi_2\left(\begin{matrix}q^{-2n},b,c\\b^{-1}q^{2-2n},c^{-1}q^{2-2n}\end{matrix};\frac{q^{3-n}}{bc}\right)\\&=\frac{(q^{-2n})_n(b^{-1}c^{-1}q^{2-2n})_n}{(b^{-1}q^{1-2n})_n(c^{-1}q^{1-2n})_n}q^{3n}\frac{(1-b^{-1}q^{1-2n})(1-c^{-1}q^{1-2n})}{(1-b^{-1}q)(1-c^{-1}q)},\end{aligned} \tag{11}$$

$$\begin{aligned}&{}_3\varphi_2\left(\begin{matrix}q^{-2n},b,c\\b^{-1}q^{2-2n},c^{-1}q^{2-2n}\end{matrix};\frac{q^{2-n}}{bc}\right)\\&=\frac{(q^{-2n})_n(b^{-1}c^{-1}q^{2-2n})_n}{(b^{-1}q^{1-2n})_n(c^{-1}q^{1-2n})_n}q^{n}\frac{(1-b^{-1}q^{1-2n})(1-c^{-1}q^{1-2n})}{(1-b^{-1}q)(1-c^{-1}q)}.\end{aligned} \tag{12}$$

Proof. Jackson's identities (1) and (2) follow from the q-analog of Whipple's theorem ([6]):

$$\begin{aligned}&{}_8\varphi_7\left(\begin{matrix}a,q\sqrt{a},-q\sqrt{a},b,c,d,e,q^{-n}\\\sqrt{a},-\sqrt{a},aq/b,aq/c,aq/d,aq/e,aq^{n+1}\end{matrix};\frac{a^2q^{2+n}}{bcde}\right)\\&=\frac{(aq)_n(aq/bc)_n}{(aq/b)_n(aq/c)_n}{}_4\varphi_3\left(\begin{matrix}aq/de,b,c,q^{-n}\\bcq^{-n}/a,aq/d,aq/e\end{matrix};q\right).\end{aligned} \tag{13}$$

This equation also implies the Rogers–Ramanujan identities and plays a key role in many of Ramanujan's identities.

If we set $a=q^{-2n}$ in (12) we obtain

$$\begin{aligned}&{}_5\varphi_4\left(\begin{matrix}q^{-2n},b,c,d,e\\b^{-1}q^{1-2n},c^{-1}q^{1-2n},d^{-1}q^{1-2n},e^{-1}q^{1-2n}\end{matrix};\frac{q^{2-3n}}{bcde}\right)\\&=\frac{(q^{-2n})_n(b^{-1}c^{-1}q^{1-2n})_n}{(b^{-1}q^{1-2n})_n(c^{-1}q^{1-2n})_n}{}_4\varphi_3\left(\begin{matrix}d^{-1}e^{-1}q^{1-2n},b,c,q^{-n}\\bcq^n,d^{-1}q^{1-2n},e^{-1}q^{1-2n}\end{matrix};q\right).\end{aligned} \tag{14}$$

Equation (1) is the case $bcde=q^{1-3n}$. Equation (2) is the case $de=q^{1-2n}$.

To obtain identities for almost poised but not well-poised series, we start with an almost poised version of (13) (see [1], Corollary 4.1):

$$
{}_6\varphi_5\left(\begin{matrix}a, b, c, d, e, q^{-n} \\ a/b, a/c, aq/d, aq/e, aq^n\end{matrix}; \frac{a^2q^{1+n}}{bcde}\right) - \frac{(1-b)(1-c)(1-q^n)}{(1-a/b)(1-a/c)(1-aq^n)}\left(\frac{a^2}{bc}\right)
$$

$$
{}_6\varphi_5\left(\begin{matrix}a, bq, cq, d, e, q^{1-n} \\ aq/b, aq/c, aq/d, aq/e, aq^{n+1}\end{matrix}; \frac{a^2q^{2+n}}{bcde}\right)
$$

$$
= \frac{(a)_n(a/bc)_n}{(a/b)_n(a/c)_n}\,{}_4\varphi_3\left(\begin{matrix}aq/de, b, c, q^{-n} \\ bcq^{1-n}/a, aq/d, aq/e\end{matrix}; q\right). \tag{15}
$$

Again setting $a = q^{-2n}$ gives us

$$
{}_5\varphi_4\left(\begin{matrix}q^{-2n}, b, c, d, e \\ b^{-1}q^{-2n}, c^{-1}q^{-2n}, d^{-1}q^{1-2n}, e^{-1}q^{1-2n}\end{matrix}; \frac{q^{1-3n}}{bcde}\right)
$$

$$
= \frac{(q^{-2n})_n(b^{-1}c^{-1}q^{-2n})_n}{(b^{-1}q^{-2n})_n(c^{-1}q^{-2n})_n}\,{}_4\varphi_3\left(\begin{matrix}d^{-1}e^{-1}q^{1-2n}, b, c, q^{-n} \\ bcq^{1+n}, d^{-1}q^{1-2n}, e^{-1}q^{1-2n}\end{matrix}; q\right). \tag{16}
$$

Equation (3) is the case $bcde = q^{-3n}$. Equation (4) is the case $de = q^{1-2n}$.

The remaining identities follow from a formula given by I Goulden and the present author [4] for the constant term with respect to x_1, x_2 and x_3 in

$$
f(x_1, x_2, x_3) = (x_1/x_2)_\alpha (qx_2/x_1)_\alpha (x_1/x_3)_a (qx_3/x_1)_\beta (x_2/x_3)_b (qx_3/x_2)_\gamma, \tag{17}
$$

where

$$
0 \leqslant b - \alpha \leqslant 1,
$$

and

$$
|\beta - \gamma| \leqslant 1.
$$

By the q-binomial theorem ([2]; Theorem 2.1) we have

$$
(z)_a(q/z)_b = \sum (-1)^i q^{i(i-1)/2} z^i \frac{(q)_{a+b}}{(q)_{a-i}(q)_{b+i}}, \quad -b \leqslant i \leqslant a. \tag{18}
$$

The function $f(x_1, x_2, x_3)$ can thus be expressed as a triple summation

$$
f(x_1, x_2, x_3) = \sum x_1^{i+j} x_2^{-i+k} x_3^{-j-k} (-1)^{i+j+k} q^{i(i-1)+j(j-1)+k(k-1))/2} *
$$

$$
* \frac{(q)_{a+\alpha}(q)_{a+\beta}(q)_{b+\gamma}}{(q)_{a-i}(q)_{\alpha+i}(q)_{a-j}(q)_{\beta+j}(q)_{b-k}(q)_{\gamma+k}}. \tag{19}
$$

Setting $i = -j = k$ yields the constant term which, after simplification, can be expressed as

$$
\text{C.T. } f(x_1, x_2, x_3) = \frac{(q)_{a+\alpha}(q)_{a+\beta}(q)_{b+\gamma}(-1)^a q^{a(3a+1)/2}}{(q)_{2a}(q)_{a+\beta}(q)_{a+b}(q)_{\alpha-a}(q)_{\gamma-a}} *
$$

$$
* {}_3\varphi_2\left(\begin{matrix}q^{-2a}, q^{-a-\beta}, q^{-a-b} \\ q^{\alpha-a+1}, q^{\gamma-a+1}\end{matrix}; q^{a+\beta+b+1}\right), \tag{20}
$$

where C.T. denotes constant term with respect to x_1, x_2 and x_3.

We shall equate this with the expression given for the constant term given in Proposition 2.4 of [4].

Let $S(\delta, \varepsilon, \varphi)$ where $\delta, \varepsilon, \varphi \in \{0, 1\}$ be the set of bijections σ from $\{1, 2, 3\}$ to $\{a, b, c\}$ such that

(i) if $\delta = 1$, then $\sigma^{-1}(a) < \sigma^{-1}(b)$,
(ii) if $\varepsilon = 1$, then $\sigma^{-1}(a) < \sigma^{-1}(c)$, and
(iii) if $\varphi = 1$, then $\sigma^{-1}(b) < \sigma^{-1}(c)$.

Let $I(\sigma)$ be $(3 - \sigma^{-1}(c))c$, if $\sigma^{-1}(a) < \sigma^{-1}(b)$ and

$$b + (3 - \sigma^{-1}(c))c, \quad \text{if } \sigma^{-1}(a) > \sigma^{-1}(b).$$

We define $F(\delta, \varepsilon, \varphi)$ to be

$$F(\delta, \varepsilon, \varphi) = \sum \frac{q^{I(\sigma)}}{(1 - q^{\sigma(1)})(1 - q^{\sigma(1)+\sigma(2)})}, \quad \sigma \in S(\delta, \varepsilon, \varphi). \tag{21}$$

As examples, we have

$$F(1,0,0) = \frac{1}{(1-q^a)(1-q^{a+b})} + \frac{q^c}{(1-q^a)(1-q^{a+c})} + \frac{q^{2c}}{(1-q^c)(1-q^{a+c})}$$

$$= \frac{1 - q^{a+b+c}}{(1-q^a)(1-q^c)(1-q^{a+b})}, \tag{22}$$

$$F(0,1,0) = \frac{1}{(1-q^a)(1-q^b)} + \frac{q^c}{(1-q^a)(1-q^{a+c})}, \tag{23}$$

$$F(1,0,1) = \frac{1}{(1-q^a)(1-q^{a+b})}, \tag{24}$$

$$F(1,1,0) = \frac{1}{(1-q^a)(1-q^{a+b})} + \frac{q^c}{(1-q^a)(1-q^{a+c})}. \tag{25}$$

Letting $c = \max(\beta, \gamma)$, Proposition 2.4 of [4] implies that

$$\text{C.T. } f(x_1, x_2, x_3) = \frac{(q)_{a+b+c-1}}{(q)_{a-1}(q)_{b-1}(q)_{c-1}} F(b - \alpha, c - \beta, c - \gamma). \tag{26}$$

Combining this with (19) and setting $B = q^{-a-b}$, $C = q^{-a-\beta}$ and $n = a$ yields

$${}_3\varphi_2\left(\begin{matrix} q^{-2n}, B, C \\ B^{-1}q^{1-2n+\alpha-b}, C^{-1}q^{1-2n+\gamma-\beta} \end{matrix}; \frac{q^{1-n}}{BC}\right)$$

$$= \frac{(q^{-2n})_n (B^{-1}C^{-1}q^{1-2n+\gamma-\beta})_n}{(B^{-1}q^{1-2n+\alpha-b})_n (C^{-1}q^{1-2n+\gamma-\beta})_n} \frac{(q)_{a+b}}{(q)_{n+\alpha}} F(b - \alpha, c - \beta, c - \gamma). \tag{27}$$

This is valid for $B = q^{-a-b}$, b any integer larger than a, and $C = q^{-1-\beta}$, β any integer larger than a. Since it is equivalent to a polynomial identity in B^{-1} and C^{-1}, it is valid for all values of B and C.

Equation (5) is the case $\alpha = b - 1$, $\beta = \gamma = c$. Equation (6) is the case $\alpha = b$, $\beta + 1 = \gamma = c$ with variables replaced by their inverses and the order of summation reversed. Equation (7) is the case $\alpha = b - 1$, $\beta + 1 = \gamma = c$. Equations (2) and (4) are also special cases of equation (27).

Conclusions and questions

Comparing (2), (4) and (5), one is struck by their similarity. Are there any other similar identities with the same simplicity?

What are the almost poised versions of the q-analog of Whipple's theorem which correspond to (5), (6) and (7)?

Can (1) and (3) be restated as constant term identities in a manner as simple as that used for (5)–(7)?

The proof of (15) is easily generalized to obtain identities in which two of the denominator parameters are of the form aq^i/b, aq^i/c, where i is an arbitrary integer. These identities, however, look immensely complicated. Can they be restated in a simple form?

What other almost poised identities exist?

References

[1] Agarwal A K, Andrews G E and Bressoud D M, The Bailey lattice, *J. Indian Math. Soc.* (to appear)
[2] Andrews G E, *The theory of partitions* (Reading, Mass: Addison–Wesley) (1976)
[3] Bailey W N. *Hypergeometric series*, reprinted by Hafner, New York (1972)
[4] Bressoud D M and Goulden I E, Constant term identities extending the q-Dyson theorem. *Trans. Am. Math. Soc.* **29** (1985) 203–228
[5] Jackson F H, Certain q-identities, *Q. J. Math.* **12** (1941) 167–172
[6] Watson G N, A new proof of the Rogers–Ramanujan identities, *J. London Math. Soc.* **4** (1929) 4–9

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 67–74.
©Printed in India.

On Whittaker models and the vanishing of Fourier coefficients of cusp forms†

STEPHEN GELBART* and DAVID SOUDRY**

* Department of Mathematics, The Weizmann Institute of Science, Rehovot 76100, Israel
** Department of Mathematics, Tel-Aviv University, Tel Aviv 69978, Israel

Abstract. The purpose of this paper is to construct examples of automorphic cuspidal representations which possess a ψ-Whittaker model even though their ψ-Fourier coefficients vanish identically. This phenomenon was known to be impossible for the group $GL(n)$, but in general remained an open problem. Our examples concern the metaplectic group and rely heavily upon J L Waldspurger's earlier analysis of cusp forms on this group.

Keywords. Whittaker models; cusp forms; automorphic cuspidal representations.

1. Introduction

Consider the following:

Question: Do there exist automorphic cuspidal representations which are *ψ-non-degenerate* and yet not *ψ-generic*? i.e. can there exist an automorphic cuspidal representation which possesses an (abstract) ψ-Whittaker model and yet the Whittaker model consisting of its ψ-th Fourier coefficients vanishes identically?

For $G = GL(n)$, the answer to this question is "no", since any automorphic cuspidal representation is automatically ψ-generic, for any $\psi \not\equiv 1$. Indeed, the ψ-Fourier coefficients of a cusp form on $GL(n)$ are known to completely determine the form; cf. ([9], p. 302, [13]).

The purpose of this paper is to show that the answer to the *question* in general is "yes". We do this by treating the special case of the metaplectic group $\widetilde{SL}_2(\mathbb{A})$ where we can appeal to Waldspurger's profound analysis of the space of cusp forms. The expert will observe that almost all the ingredients of our proof can be found in (one place or another in) [16], [17]. Our contribution has been to focus attention on the Whittaker model question posed above, and to answer it by reformulating Waldspurger's theory.

To describe our result, let us fix once and for all a nontrivial character ψ of $F\backslash\mathbb{A}$, and regard $\widetilde{SL}_2$ as part of the dual reductive pair $(\widetilde{SL}_2, PGL_2)$ in the sense of [6]. The Shimura–Shintani correspondence of [16] then provides a bijection between the set of irreducible automorphic cuspidal representations σ of $\widetilde{SL}_2(\mathbb{A})$ which have non-

† This research was partially supported by Grant No. 8400139 from the United States–Israel Bi National Science Foundation (BSF), Jerusalem, Israel.

vanishing ψ-Fourier coefficients and the set of irreducible automorphic cuspidal representations π of $PGL_2(\mathbb{A})$ satisfying $L(\pi, \frac{1}{2}) \neq 0$. In § 2 we describe how the domain of this bijection may be extended (via Howe's correspondence) to include all σ which "merely" possess an abstract ψ-Whittaker functional; the resulting image then consists of all irreducible automorphic cuspidal π with $\varepsilon(\pi, \frac{1}{2}) = 1$. In other words, the cuspidal representations whose existence is questioned in our "problem" above are precisely the Howe lifts of π on $PGL_2(\mathbb{A})$ with

$$L(\pi, \tfrac{1}{2}) = 0 \quad \text{and} \quad \varepsilon(\pi, \tfrac{1}{2}) = 1.$$

In order to show that such representations π exist, we give some examples in § 3. Finally, in § 3, we include some remarks about the possibility of finding similar examples for other groups (and other dual reductive pairs).

We are grateful to D Ramakrishnan for prodding us to think seriously about this question. It is also a pleasure to thank J Bernstein, I Piatetski-Shapiro and P Sarnak for encouraging remarks, Ruby Musrie for her speedy job of preparing the manuscript, and the Institute for Advanced Studies in Jerusalem for its hospitality.

2 The relation between the correspondences of Howe and Waldspurger

2.1 We begin by recalling the key results of [16] needed in this paper. For a detailed analysis of Waldspurger's theory, or assistance with unexplained facts or terminology, the reader is referred to [10] and [4].

Let A_{oo} denote the space of genuine cusp forms on $\widetilde{SL_2}(\mathbb{A})$ orthogonal to all theta-series in one-variable. For any irreducible automorphic cuspidal representation $\sigma = \otimes \sigma_v$ appearing in A_{oo}, there is attached an irreducible subspace

$$\pi = \theta(\sigma, \psi)$$

of the space of cusp forms on $PGL_2(\mathbb{A})$; this is the "theta-series lift" of σ to PGL_2. Conversely, given any irreducible automorphic cuspidal representation $\pi = \otimes \pi_v$ of $PGL_2(\mathbb{A})$, its theta-series lifting $\theta(\pi, \psi)$, defines an irreducible subspace of A_{oo}. We recall that these maps are adelizations of Shintani and Niwa's treatment of *Shimura's correspondence in* [14]. According to the theory of [16]:

(a) There are local analogues of the correspondences above, such that

$$\theta(\sigma, \psi) = \otimes\, \theta(\sigma_v, \psi_v)$$

and

$$\theta(\pi, \psi) = \otimes\, \theta(\pi_v, \psi_v);$$

moreover, these local correspondences are defined (and non-zero) for arbitrary local σ_v and π_v (provided σ_v is ψ_v-non-degenerate);

(b) $\theta(\sigma, \psi) \equiv \{0\}$ if and only if the ψ-Fourier coefficient of any cusp form in the space of σ is zero;

(c) $\theta(\pi, \psi) \equiv \{0\}$ if and only if $L(\pi, \frac{1}{2}) = 0$.

Remarks

(i) Let $A_{oo}(\psi)$ be the space of cusp forms on $\widetilde{SL_2}(\mathbb{A})$ with non-vanishing ψ-Fourier coefficients. Then $\sigma \to \theta(\sigma, \psi)$ defines a bijection between the set of irreducible σ in $A_{oo}(\psi)$ and the set of irreducible cuspidal representations π of $PGL_2(\mathbb{A})$ such that $L(\pi, \frac{1}{2}) \neq 0$.

(ii) If ψ' is another non-trivial character of $F\backslash\mathbb{A}$ such that σ belongs to $A_{oo}(\psi')$ as well as $A_{oo}(\psi)$, then there exists b in F^x such that $\psi' = \psi^b$ and

$$\theta(\sigma, \psi') = \theta(\sigma, \psi) \otimes \chi_b$$

(with χ_b the quadratic character of $F^x\backslash\mathbb{A}^x$ associated to $F(\sqrt{b})$; cf. Prop. 28 of [16]). Thus one can extend the correspondence $\sigma \to \theta(\sigma, \psi)$ *to all irreducible constituents of* A_{oo} by defining

$$\sigma \to Wd(\sigma, \psi) = \theta(\sigma, \psi^b) \otimes \chi_b$$

for any ψ^b such that $\theta(\sigma, \psi^b) \neq \{0\}$. The image of this extended map consists of all irreducible automorphic cuspidal representations π of $PGL_2(\mathbb{A})$ such that

$$L(\pi \otimes \chi_b, \tfrac{1}{2}) \neq 0$$

for *some* b in F^x. (cf. [17], Prop. 19 and Cor. 1; also p. 300 of [10].) The problem with this extended correspondence is that *it is no longer one-to-one.*

2.2 Implicit in our discussion above is the fact that σ appears in A_{oo} with multiplicity one, i.e. in defining the correspondence $Wd(\sigma, \psi)$, we may indeed confuse σ with the space of cusp forms realizing it. Waldspurger derives this multiplicity one result as a Corollary of the assertion that the non-vanishing of the ψ-Fourier coefficients of cusp forms in the space of σ depends only on σ as an abstract representation. More precisely, these coefficients are non-zero if and only if each σ_v is ψ_v-non-degenerate *and* $L(Wd(\sigma, \psi), \frac{1}{2}) \neq 0$. This last assertion then suggests a strategy for finding ψ-non-degenerate σ with trivial ψ-Fourier coefficients: restrict $Wd(\sigma, \psi)$ to the set of ψ-non-degenerate σ in A_{oo}, and try to prove that this restriction is an injection (with image containing π such that $L(\pi, \frac{1}{2}) = 0$).

To this end, let $D(\psi) \supseteq A_{oo}(\psi)$ denote those σ in A_{oo} which support a non-trivial ψ-Whittaker functional. (For the time being, we do not know that $D(\psi)$ properly contains $A_{oo}(\psi)$; it is the purpose of this paper to show this.) Consider also the *local* correspondences

$$\begin{aligned} &\sigma_v \to \theta(\sigma_v, \psi_v) \\ &\pi_v \to \theta(\pi_v, \psi_v) \end{aligned} \tag{1}$$

described in § 2.1(a). These correspondences are precisely *concrete* (non-zero) realizations of the *abstract* "θ-series liftings" defined in [6], i.e. $\mathrm{Hom}_{\widetilde{SL_2}(F_v) \times PGL_2(F_v)}(r_{\psi}, \sigma_v \otimes \pi_v) \neq 0$ if and only if $\pi_v = \theta(\sigma_v, \psi_v)$ or $\sigma_v = \theta(\pi_v, \psi_v)$, with σ_v non-degenerate with respect to ψ_v. Thus, given *any* $\sigma = \otimes \sigma_v$ in $D(\psi)$, it is natural to consider the abstract

representation

$$H(\sigma,\psi)=\otimes\theta(\sigma_v,\psi_v) \tag{2}$$

of $PGL_2(\mathbb{A})$.

Note that (2) defines a non-trivial representation of $PGL_2(\mathbb{A})$ independently of the vanishing of $\theta(\sigma,\psi)$; all that matters is that σ_v possess an abstract ψ_v-Whittaker model for every v. We call $H(\sigma,\psi)$ the *Howe lifting* of σ to $PGL_2(\mathbb{A})$. This lifting is clearly one-to-one, but it does not *apriori* preserve "automorphicity". If σ is such that $\theta(\sigma,\psi)$ already defines a non-trivial representation, i.e. σ belongs to $A_{oo}(\psi)$, then $H(\sigma,\psi)=\theta(\sigma,\psi)$; hence $H(\sigma,\psi)$ is obviously automorphic cuspidal in this case. In general, we have the following:

Theorem. *For each σ in $D(\psi)$, $\pi=H(\sigma,\psi)$ is an irreducible automorphic cuspidal representation of $PGL_2(\mathbb{A})$ with the property that*

$$\varepsilon(\pi,\tfrac{1}{2})=1. \tag{3}$$

Conversely, if π is any irreducible automorphic cuspidal representation of $PGL_2(\mathbb{A})$ satisfying (3), *then its Howe lift*

$$H(\pi,\psi)\equiv\otimes\theta(\pi_v,\psi_v)$$

is automorphic cuspidal on $\overline{SL_2}(\mathbb{A})$ and belongs to $D(\psi)$; moreover,

$$H(H(\pi,\psi),\psi)=\pi$$

and

$$H(H(\sigma,\psi),\psi)=\sigma.$$

Proof. Consider the cuspidal representation $\pi'=Wd(\sigma,\psi)\equiv\theta(\sigma,\psi^{\xi})\otimes\chi_{\xi}$ with σ in $D(\psi)$. Locally, for any v,

$$\pi'_v=\theta(\sigma_v,\psi_v^{\xi})\otimes\chi_{\xi,v}=\theta(\sigma_v,\psi_v) \tag{4}$$

since σ_v, by assumption, has a ψ_v-Whittaker model. (This is the local analogue of the result quoted in Remark 2.1(ii) above; it is proved in [17]). Hence

$$\pi=\otimes H(\sigma_v,\psi_v)=\otimes\theta(\sigma_v,\psi_v)=\pi'=Wd(\sigma,\psi)$$

is indeed automorphic cuspidal. Moreover, since π is in the image of Wd, we know $L(\pi\otimes\chi_{\xi},\tfrac{1}{2})\neq 0$ for some $\xi\in F^x$ (again see Remark (2.1)(ii) above); on the other hand equation (4) implies

$$\theta(\pi_v\otimes\chi_{\xi,v},\psi_v^{\xi})=\sigma_v$$

for each v. Therefore (by Theorem 2.5 and the "Additional note" on p. 301 of [10]) we may conclude $\varepsilon(\pi,\tfrac{1}{2})=1$.

Conversely, suppose π cuspidal on $PGL_2(\mathbb{A})$ satisfies $\varepsilon(\pi,\tfrac{1}{2})=1$. Then directly from Theorem A.1 of [10] (together with the "Additional note" on p. 301) we conclude

$\sigma = H(\pi, \psi) = \otimes \theta(\pi_v, \psi_v)$ is automorphic cuspidal, belongs to $D(\psi)$, and maps back to π under the inverse Howe lifting $\otimes \theta(\sigma_v, \psi_v)$.

Remark.

The fact that $H(\pi, \psi)$ is automorphic cuspidal is not at all obvious. Indeed, if $\varepsilon(\pi, \frac{1}{2}) \neq 1$, then $H(\pi, \psi)$ is *not* automorphic.

COROLLARY 1.

The restriction of $Wd(\sigma, \psi)$ *to* $D(\psi) \supset A_{oo}(\psi)$ *remains a bijection.*
Indeed the proof of the Theorem shows that $Wd(\sigma, \psi) = H(\sigma, \psi)$ on $D(\psi)$.

COROLLARY 2.

The irreducible automorphic cuspidal representations of $\widetilde{SL_2}(\mathbb{A})$ *which are* ψ*-non-degenerate but not* ψ*-generic are precisely the Howe lifts of cuspidal* π *on* $PGL_2(\mathbb{A})$ *satisfying*

$$\varepsilon(\pi, \tfrac{1}{2}) = 1 \quad \textit{and} \quad L(\pi, \tfrac{1}{2}) = 0.$$

Indeed, the Howe correspondence and the θ-lifting correspondence $\theta(\cdot, \psi)$ agree on the domains $A_{oo}(\psi)$ and $\{\pi : L(\pi, \frac{1}{2}) \neq 0\}$. Thus our Theorem implies that the Howe correspondence is a bijection between the complements of these domains in $D(\psi)$ and $\{\pi : \varepsilon(\pi, \frac{1}{2}) = 1\}$, i.e. a bijection between the types of representations σ and π described in the Corollary.

Remark.

Recall that $Wd : \sigma \to \pi$ is not 1-1 on all of A_{oo} (see [17], [10] or [4] for a detailed description of $Wd^{-1}(\pi)$). The significance of the Howe lifting $H(\pi, \psi)$ is that for π satisfying

$$\varepsilon(\pi, \tfrac{1}{2}) = 1 \quad \text{and} \quad L(\pi, \tfrac{1}{2}) = 0$$

it picks out exactly the *one* σ in $Wd^{-1}(\pi)$ which possesses a ψ-Whittaker model. It remains therefore to exhibit π on $PGL_2(\mathbb{A})$ satisfying these conditions.

3. Examples of cuspidal π on $PGL_2(\mathbb{A})$ satisfying $L(\pi, \frac{1}{2}) = 0$ and $\varepsilon(\pi, \frac{1}{2}) = 1$

The first example is over $F = \mathbb{Q}$ and requires the theory of elliptic curves.

Example 2.1 Suppose E is an elliptic curve over $\mathbb{Q}$ with complex multiplication. Then there exists an automorphic cuspidal representation π_E of $PGL_2(\mathbb{A})$ such that $L(\sigma, \pi_E)$ is equal to the Hasse-Weil zeta-function $L(s, E)$; moreover, the (weak form of the) Birch-Swinnerton-Dyer conjecture holds for $L(s, E)$ (cf. [1]). Let us suppose also that

(i) the functional equation for E is "even", i.e. $L(s, E) = L(1 - s, E)$, and
(ii) $|E(\mathbb{Q})|$ is infinite, i.e. the rank of the Mordell-Weil group of E is positive.

Condition (i) implies that $\varepsilon(\pi, \frac{1}{2}) = 1$, whereas condition (ii) implies (by Coates-Wiles) that $L(\pi, \frac{1}{2}) = 0$.

Our second example is more elementary, but not defined over $\mathbb{Q}$.

Example 2.2. Let $\tau = \otimes \tau_v$ be an automorphic cuspidal representation $PGL_2(\mathbb{A}_F)$ satisfying the conditions:

(i) τ_v belongs to the principal series for all v; and
(ii) $\varepsilon(\tau, \frac{1}{2}) = -1$ (and hence $L(\tau, \frac{1}{2}) = 0$, by the functional equation $L(\tau, s) = \varepsilon(\tau, s)L(\tau, 1-s)$).

Such a representation τ is constructed in [10] (bottom of p. 300) by assuming F is an imaginary quadratic extension of $\mathbb{Q}$ and base change lifting a classical holomorphic cusp form with respect to $SL_2(\mathbb{Z})$. (The significance of τ is that its Howe lifting to $\widetilde{SL_2}(\mathbb{A})$ is *not* automorphic, let alone cuspidal, since $\varepsilon(\tau, \frac{1}{2}) = -1$.)

PROPOSITION.

Let K be a quadratic extension of F, and π the base change lift of τ to $PGL_2(\mathbb{A}_K)$. Then

$$L(\pi, \tfrac{1}{2}) = 0 \quad \textit{and} \quad \varepsilon(\pi, \tfrac{1}{2}) = 1.$$

Proof. Let $\chi = \otimes \chi_v$ be the quadratic character of $\mathbb{A}^x$ associated to K over F. Then we know (cf. [8]) that

$$\varepsilon(\pi, s) = \varepsilon(\tau, s)\varepsilon(\tau \otimes \chi, s)$$

and

$$L(\pi, s) = L(\tau, s)L(\tau \otimes \chi, s).$$

Thus $L(\pi, \frac{1}{2}) = 0$, since $L(\tau, \frac{1}{2}) = 0$. On the other hand, since τ_v belongs to the principal series for all v, there are quasicharacters μ_v of F_v^x such that $\tau_v = \pi(\mu_v, \mu_v^{-1})$ for each v; hence

$$\varepsilon(\tau_v, \tfrac{1}{2}) = \varepsilon(\mu_v, \tfrac{1}{2})\varepsilon(\mu_v^{-1}, \tfrac{1}{2}) = \mu_v(-1),$$

$$\varepsilon(\tau_v \otimes \chi_v, \tfrac{1}{2}) = \varepsilon(\mu_v\chi_v, \tfrac{1}{2})\varepsilon(\mu_v^{-1}\chi_v, \tfrac{1}{2}) = \mu_v\chi_v(-1),$$

and

$$\begin{aligned}\varepsilon(\pi, \tfrac{1}{2}) &= \prod_v \varepsilon(\tau_v, \tfrac{1}{2})\varepsilon(\tau_v \otimes \chi_v, \tfrac{1}{2}) \prod_v \chi_v(-1) \\ &= \chi(-1) = 1\end{aligned}$$

as claimed.

Remarks.

(i) We recall that the base change lift of an automorphic cuspidal representation τ of $PGL_2(\mathbb{A})$ fails to be cuspidal only if τ is of the form $\pi(\eta)$ with η a character of

$K^\times \backslash \mathbb{A}_K^\times$ such that $\bar{\eta} \neq \eta$. Thus the π in our Proposition is indeed cuspidal, since "τ_v principal series for all v" precludes the possibility that τ be such a $\pi(\eta)$.

(ii) The idea of executing a sequence of *consecutive* (quadratic) base changes in order to produce interesting examples of automorphic forms comes from [2].

4. Concluding remarks

How general is the phenomenon described by the examples in this paper? i.e. for which quasi-split reductive groups G are there automorphic cuspidal representations σ such that, for some "non-degenerate" character ψ of the maximal unipotent subgroup U of G, σ admits a ψ-Whittaker model, and yet the ψ-Fourier coefficients of cusp forms in the space of σ vanish identically?

4.1 Note that for the group $\overline{SL_2}$, there is more than one orbit of non-trivial characters ψ with respect to the natural action of the maximal torus. In cases where the maximal torus *does* act transitively on non-degenerate ψ (i.e. ψ such that the restriction to any simple root subgroup in U is non-trivial), Piatetski-Shapiro has formalized the notion of an automorphic cuspidal representation σ being *hypercuspidal* (cf. [11]). This means precisely that all the Fourier coefficients of σ along U (with respect to any ψ) vanish identically. By contrast, σ is called *generic* if it is orthogonal to all hypercusp forms. Clearly σ generic implies σ admits a non-trivial (abstract) Whittaker model with respect to one (and hence all) ψ. However, it is also clearly suggested now that the converse need not be true. It would be desirable, therefore, to construct examples of hypercusp forms which are non-degenerate. For the group $U_{2,1}$, these notions are discussed in [3]. It is shown there that hypercuspidal σ do exist, but the examples (constructed by way of Weil's representation) have no Whittaker models at all. This is also the case for the "Saito-Kurokawa" cusp forms constructed in [12] by way of the dual pair $(PGSp_4, \overline{SL_2})$; cf. the last section of [17].

4.2 It seems natural that more dual reductive pair liftings be studied in the spirit of Waldspurger's work. Two natural candidates are $(Sp_4,\ O_{2,2})$ and $(GSp_4, GSO(6))$, examples already examined carefully in [5] (resp. [7], [18] and [15]). Note that GSp_4 satisfies the transitivity condition alluded to in §4.1. Only for the pair $(\overline{SL_2}, PGL_2)$, however, is the θ-series lifting sufficiently well understood to be able to resolve the Whittaker model question discussed in this paper.

References

[1] Coates J and Wiles A, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977) 223–251

[2] Cogdell J and Piatetski-Shapiro I, Base change for $\overline{SL_2}$, *J. Number Theory* (to appear)

[3] Gelbart S and Piatetski-Shapiro I, Automorphic forms and *L*-functions for the unitary group, in: *Lie group representations II, Lecture notes in mathematics* No. 1041 (Berlin, Heidelberg: Springer Verlag) (1984) pp. 141–184

[4] Gelbart S and Piatetski-Shapiro I, Some remarks on metaplectic cusp forms and the correspondences of Shimura and Waldspurger, *Isr. J. Math.* **44** (1983) 97–126

[5] Howe R and Piatetski-Shapiro I, Some examples of automorphic forms on $Sp(4)$, *Duke Math. J.* **50** (1983) 55–106

[6] Howe R, θ-series and invariant theory, *Proc. Symp. Pure Math.* No. 33, Part I (Providence, RI: Am. Math. Soc.) (1979) 275–286
[7] Jacquet H, Piatetski-Shapiro I and Shalika J, The θ-correspondence from $GSp(4)$ to $GL(4)$ (in preparation)
[8] Langlands R P, Base change for $GL(2)$, *Ann. Math. Stud.* No. 96 (Princeton: University Press) (1980).
[9] Piatetski-Shapiro I, Euler subgroups, in: *Lie groups and their representations* (ed.) I M Gelfand (New York: Halsted Press) (1975)
[10] Piatetski-Shapiro I, Work of Waldspurger, in: *Lie group representations II, Lecture notes in mathematics* No. 1041 (Berlin, Heidelberg: Springer Verlag) (1984) pp. 280–302
[11] Piatetski-Shapiro I, Multiplicity one theorems, *Proc. Symp. Pure Math.* No. 33, Part I (Providence, RI: Am. Math. Soc.) (1979) 209–212
[12] Piatetski-Shapiro I, On the Saito-Kurokawa lifting, *Invent. Math.* **71** (1983) 309–338
[13] Shalika J, The multiplicity one theorem for $GL(n)$, *Ann. Math.* **100** (1974) 171–193
[14] Shimura G, On modular forms of half-integral weight, *Ann. Math.* **97** (1973) 440–481
[15] Soudry D, A uniqueness theorem for representations of $GSO(6)$ and the strong multiplicity one theorem for generic representations of $GSp(4)$, *Isr. J. Math.* **58** (1987) 257–287
[16] Waldspurger J, Correspondence de Shimura, *J. Math. Pure Appl.* **59** (1980) 1–133
[17] Waldspurger J, Correspondences de Shimura et quaternions, (preprint) (1982)
[18] Waldspurger J, Un exercise sur $GSp(4, F)$ et les representations de Weil, *Bull. Soc. Math. France* **115** (1987) 35–69

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 75–84.
© Printed in India.

On prime representing polynomials

EMIL GROSSWALD
Department of Mathematics, Temple University, Computer Building 038-16, Philadelphia, Pennsylvania 19122, USA

Abstract. A heuristic method is presented to determine the number of primes $p \leqslant x$, represented by an irreducible polynomial $f(n)$, without non-trivial fixed factor ($f(y) \in Z[y]$; $n \in Z$). The method is applied to two specific polynomials and the results are compared with those of the heuristic approach of Hardy and Littlewood.

Keywords. Primes; polynomials.

1. Introduction

In volume 2 of Ramanujan's Notebooks [4], on page 308 we find lists of primes in certain arithmetic progressions. On page 319 of the same Notebook we find actual counts of primes in different arithmetic progressions to the same modulus. In several instances, Ramanujan studies the representation of primes, belonging to given residue classes of certain moduli, as quadratic forms in 2 variables. Hence, Ramanujan considered primes represented by first degree polynomials in one variable and by second degree polynomials in two variables. Did he ever consider the representation of primes by second degree polynomials in one variable, e.g. by $y^2 + 1$? If he ever did, he did not transcribe anything on that topic in his known notebooks. It is at least conceivable that the difficulty of the subject prevented him from obtaining results that he should consider worthwhile recording. In fact, this problem is still unsolved at present and only conjectural results exist. Did Ramanujan ever discuss this matter with Hardy? This we shall, presumably never know, unless some new, at present "lost" documentary evidence appears sometime in the future.

Be that as it may, it is a fact that shortly after Ramanujan's death, Hardy and Littlewood's famous paper appeared on problems of Partitio Numerorum, Part III [2]. In it the number $N(n)$ of primes $p \leqslant n$, of the form $y^2 + 1$ is discussed. As the authors state, they prove no theorem on this subject, not even a conditional one (i.e. one that assumes the validity of some unproved hypothesis). What they come up with, by using the circle method, earlier developed by Hardy and Ramanujan, is a conjectural asymptotic *formula* for $N(n)$. The procedure is formal and error terms are ignored.

This conjectural result is the following:
Denote by $N(n)$ the number of primes $p \leqslant n$ and of the form $p = y^2 + 1$ and set $C = \prod_{p \geqslant 3} (1 - (-1/p)(p-1)^{-1})$; then, as $n \to \infty$,

$$N(n) \simeq C \frac{\sqrt{n}}{\log n} = N_0(n), \quad \text{say.} \qquad (*)$$

The authors then compare the figures furnished by (*) with the actual count of primes $p = y^2 + 1 \leqslant n$ and find a most satisfactory agreement.

They generalize their approach to arbitrary, irreducible polynomials without fixed divisor and with integer coefficients, but not to such polynomials, which are integral valued, without having necessarily integer coefficients, such as, e.g. $p = \frac{1}{2}y(y+1)+1$. However, by following their method (more specifically, by use of their "Conjecture F" of [2]), it is not difficult to show that, if one now denotes by $N(n)$ the number of primes $p \leqslant n$, of the form $p = \frac{1}{2}y(y+1)+1$, one obtains

$$N(n) \simeq 2C' \frac{\sqrt{n}}{\log n} = N_0(n), \quad \text{say,} \tag{**}$$

where $C' = \lim_{x \to \infty} \prod_{p \leqslant 3} (1 - \chi(p)(p-1)^{-1})$, $\chi(p) = (p/7)$, the Legendre symbol.

In what follows, we take up once more the problem of the number of primes $p = y^2 + 1 \leqslant n$ and the corresponding one for $p = \frac{1}{2}y(y+1)+1$. We shall treat the first one in detail, the second one more briefly.

The present results are also only conjectural, but the method used is entirely different from that of Hardy and Littlewood. While they use the circle method and a weak form of the generalized Riemann hypothesis and then ignore error terms (as already recalled, they explicitly disclaim any proof and only propose a formula), we shall use a sieve method approach and propose a certain conjectural fudge factor, that should compensate for neglected error terms and also another lack of accuracy that will occur. Some numerical computations are made in order to compare the results of the different proposed formulae with actual counts of primes, but these computations are limited and all were performed on a hand calculator, so that third decimals should not be taken too seriously. While this may not be significant, it turns out that, as far as the computations go, the best fit to actual counts is obtained with the fudge factor $c = 1$.

2. Sketch of the method

Let $f(y)$ be a polynomial, integral valued, irreducible, of arbitrary degree and without non-trivial constant divisor, but not necessarily with integer coefficients. If a prime p divides $f(m)$ for a_p values of m modulo p, then the number of integers represented by $f(m)$, with $m \leqslant x$ and such that $p \nmid f(m)$ equals $x - a_p[x/p] - \varepsilon_p$, where ε_p stands for the number of solutions of $f(m) \equiv 0 (\mathrm{mod}\, p)$ on the segment $p[x/p] < m \leqslant x$: clearly, $0 \leqslant \varepsilon_p \leqslant a_p$. For simplicity and without loss of generality, we shall assume that x is an integer. By the independence of congruences modulo distinct primes, the number of integers $f(m)$ with $m \leqslant x$, such that no prime $p \leqslant z$ divides $f(m)$ equals

$$x \prod_{p \leqslant z} \left(1 - \frac{a_p}{x}[x/p] - \frac{\varepsilon_p}{x}\right) = x \prod_{p \leqslant z} \left(1 - \frac{a_p}{p} + \delta_p\right), \tag{1}$$

where $|\delta_p| \leqslant a_p/x$. In particular, if $z = \sqrt{f(x)}$, then this sieving process leaves, in principle all (and only) primes represented by $f(m)$, $m \leqslant x$, except that those primes $f(m)$ that are less than z will also have been wrongly removed. It will follow from an

easy extension of the present considerations (see especially formulae (5′) and (10)) that, if $f(m)$ is of degree h and $f(x) = n$, then our conjecture implies in particular that the number of those wrongly eliminated primes does not exceed a constant multiple of $n^{1/2h}/\log n$, which is negligible with respect to the principal term of order $n^{1/h}/\log n$. One observes, however, that formally even larger primes, up to $f(x)/2$ may be considered. In fact, even if $[x/p] = 0$, in general $\delta_p \neq 0$ and the factor $1 + \delta_p$ may affect the product. If we select z so that $\sqrt{f(x)} \leqslant z \leqslant f(x)/2$, the number of $f(m)$ that are primes does not change and (1) appears to remain valid, but the value of the product changes. This vagueness in the selection of z has been pointed out already by Hardy and Littlewood (see [2, p. 37, footnote 1]). Finally, the δ_p's, if taken in absolute value, lead to an error term that swamps the main term. In fact, however, the δ_p's are not of constant sign and it is highly unlikely that the true error term is of an order as high as that of the principal term, but no proof of this conjecture is known.

In what follows we shall ignore the δ_p's and choose $z = (f(x))^{a/2}$. It will turn out that z enters the formula for the number $\tilde{N}(x)$ of primes represented by $f(m)$ with $m \leqslant x$ in the form of a factor $1/\log z = 2/(\alpha \log f(x))$. Hence, the choice of α translates into a multiplicative coefficient α^{-1}, independent of x, for the formula of $\tilde{N}(x)$. We shall make the following *Conjecture*: For every polynomial there exists a fudge factor c, independent of x, such that, if we ignore the δ_p's and take $z = \sqrt{f(x)}$, then $\tilde{N}(x)$ is asymptotically equal to $cx \prod_{p \leqslant z} (1 - a_p/p)$.

In some respect it is more satisfactory to ask for the number $N(n)$ of primes represented by $f(m)$, when $f(m) \leqslant n$. It is clear that, if $f(x) = n$, then $\tilde{N}(x) = N(n)$.

Concerning the fudge factor, it is worthwhile to recall that some such non-trivial fudge factors are in fact needed and are well known. Let us consider, e.g. the polynomial $f(y) = y$. In this case, $a_p = 1$ for all primes. If in (1) we set $a_p = 1$, ignore the δ_p's and take $z = \sqrt{x}$, we obtain

$$\tilde{N}(x) = N(n) \simeq cx \prod_{p \leqslant \sqrt{x}} (1 - p^{-1}) \simeq cx \frac{e^{-\gamma}}{\log \sqrt{x}} \simeq 2ce^{-\gamma}(x/\log x) = 2ce^{-\gamma}(n/\log n).$$

By the prime number theorem we know that $N(n) \simeq n/\log n$; hence, the formula yields the correct result only if we use the fudge factor $c = e^{\gamma}/2 \simeq 0{\cdot}8905\ldots \neq 1$.

3. A conjectural theorem

On the basis of the preceding discussion, we state the following

Conjectural Theorem. Let $f(y)$ be an irreducible polynomial, integral-valued and without non-trivial constant divisor, but not necessarily with integer coefficients. Then the number $\tilde{N}(x)$ of primes represented by $f(m)$, $m \in \mathbb{Z}$, $0 \leqslant m \leqslant x$, satisfies

$$\tilde{N}(x) \simeq cx \prod_{p < \sqrt{f(x)}} \left(1 - \frac{a_p}{p}\right), \tag{2}$$

where c is a fudge factor, independent of x, but which may depend on the polynomial $f(y)$. Also, if $f(x) = n$, then the number of primes not exceeding n and represented by

$f(m)$, $m \in \mathbb{Z}$, is given by

$$N(n) \simeq c x_0 \prod_{p \leqslant \sqrt{n}} \left(1 - \frac{a_p}{p}\right), \tag{2'}$$

where x_0 is the solution of $f(x_0) = n$. (This solution is unique for sufficiently large n; if ay^h is the leading term of $f(y)$, then $x_0 \simeq (n/a)^{1/h}$).

The problem arises as to how to determine the value of the factor c. One approach is to consider formulae for $N(n)$ obtained by other considerations (even if only conjectural ones) and then identify them with (2'). Another approach is to compare the numerical results of the conjectured formulae, with actual counts of the primes up to n, represented by $f(y)$. Finally, one may brazenly ignore all inaccuracies and consider (2), or (2'), without any fudge factor, i.e. with $c = 1$.

From here on we shall consider only the case of quadratic polynomials (i.e. $h = 2$) and, in fact, restrict ourselves to two specific ones, $f(y) = y^2 + 1$ and $f(y) = 1 + y(y+1)/2$.

4. The polynomial $f(y) = y^2 + 1$

Let $x \in \mathbb{Z}$ be large. For odd integer m, $2 | (m^2 + 1)$, so that $m^2 + 1$ can be prime only for $m = 1$, or for m even. There are $[x/2] + 1 = (x/2) + 1 - \varepsilon_2 (\varepsilon_2 = 0$, or $1/2)$ such values $m \leqslant x$. For p odd, $m^2 + 1 \equiv 0 (\mathrm{mod}\, p)$ is possible only for $p \equiv 1 (\mathrm{mod}\, 4)$; therefore, $a_p = 0$ for $p \equiv 3 (\mathrm{mod}\, 4)$. On the other hand, if $p \equiv 1 (\mathrm{mod}\, 4)$, then there exist 2 values of $m (\mathrm{mod}\, p)$, such that $m^2 + 1 \equiv 0 (\mathrm{mod}\, p)$; hence, $a_p = 2$ for $p \equiv 1 (\mathrm{mod}\, p)$. Formula (2) becomes

$$\tilde{N}(x) \simeq c \frac{x}{2} \prod_{\substack{p \leqslant x \\ p \equiv 1 (\mathrm{mod}\, 4)}} \left(1 - \frac{2}{p}\right). \tag{3}$$

We proceed to estimate the product in (3). All congruences without indication of a modulus are understood modulo 4 (in this section only).

$$\prod_{\substack{p \leqslant x \\ p \equiv 1}} \left(1 - \frac{2}{p}\right) = \prod_{\substack{p \leqslant x \\ p \equiv 1}} \left(1 - \frac{1}{p}\right)^2 \frac{1 - 2p^{-1}}{(1 - p^{-1})^2} = \prod_{\substack{p \leqslant x \\ p \equiv 1}} \left(1 - \frac{1}{p}\right)^2 \prod_{\substack{p \leqslant x \\ p \equiv 1}} \left(1 - \frac{1}{(p-1)^2}\right).$$

As $x \to \infty$, the last product converges to a constant, say $A = \prod_{p \equiv 1} (1 - (p-1)^{-2}) \cong$ 0·927... and (3) becomes

$$\tilde{N}(x) \simeq \frac{c}{2} A x \prod_{\substack{p \leqslant x \\ p \equiv 1}} \left(1 - \frac{1}{p}\right)^2.$$

It may be shown (see [1]) that

$$\prod_{\substack{p \leqslant x \\ p \equiv 1}} \left(1 - \frac{1}{p}\right)^2 \simeq \frac{8 e^{-\gamma}}{\pi} B (\log x)^{-1},$$

where B stands for the convergent infinite product $\prod_{p \equiv 3} (1 - p^{-2})^{-1}$. This constant

appears in some work of Landau (see [3]). Its value is about 1·1680... We have obtained

$$\tilde{N}(x) \simeq c\frac{4e^{-\gamma}}{\pi}AB\frac{x}{\log x}. \tag{4}$$

Formula (4) can be simplified. In what follows, ratios of semi-convergent, or even divergent products will occur; the ratios themselves will converge. A correct writing is $\lim_{x\to\infty}\{\prod_{p<x}(\cdots)/\prod_{p\leqslant x}(\cdots)\}$. To avoid this cumbersome writing, this notation will be suppressed, although that will make the intermediate expressions formally invalid.

The constant A may be rewritten as follows:

$$\begin{aligned}
A &= \prod_{p\equiv 1}(1-(p-1)^{-1})\prod_{p\equiv 1}(1+(p-1)^{-1}) \\
&= \prod_{p\equiv 1}(1-(p-1)^{-1})\prod_{p\equiv 3}(1+(p-1)^{-1})\frac{\prod_{p\equiv 1}(1+(p-1)^{-1})}{\prod_{p\equiv 3}(1+(p-1)^{-1})} \\
&= \prod_{p\geqslant 3}\left(1-\frac{(-1/p)}{p-1}\right)\frac{\prod_{p\equiv 1}\frac{p}{p-1}}{\prod_{p\equiv 3}\frac{p}{p-1}} = C\frac{\prod_{p\equiv 3}(1-p^{-1})}{\prod_{p\equiv 1}(1-p^{-1})} = C\lim_{x\to\infty}\frac{\prod_{p\leqslant x,p\equiv 3}(1-p^{-1})}{\prod_{p\leqslant x,p\equiv 1}(1-p^{-1})}.
\end{aligned}$$

Here C stands for the semiconvergent product $\prod_{p\geqslant 3}(1-(-1/p)(p-1)^{-1})$. As $x\to\infty$, the last ratio is known to approach the constant $\pi/4B$ (see [1]), so that $A=\pi C/4B$ and $4AB/\pi = C$. It follows that (4) may be written simply as

$$\tilde{N}(x) \simeq ce^{-\gamma}C\frac{x}{\log x}. \tag{5}$$

If we replace x by n as a variable, where $n = x^2+1$, then (5) becomes

$$N(n) \simeq c\cdot 2e^{-\gamma}C\frac{\sqrt{n}}{\log n}. \tag{5'}$$

As already mentioned, Hardy and Littlewood [2] have obtained the conjectural formula

$$N(n) \simeq C\frac{\sqrt{n}}{\log n} = N_0(n) \tag{5''}$$

by an entirely different approach. This suggests that we take the fudge factor $c = e^{\gamma}/2$. For reasons that will become clear immediately, it is worthwhile to consider also

$$N(n) \simeq C_1\frac{\sqrt{n}}{\log n}, \quad \text{with} \quad C_1 = 2e^{-\gamma}C, \tag{5'''}$$

i.e. (5') with fudge factor $c=1$. We shall denote the second member of (5''') by $N_1(n)$.

5. Numerical comparisons

It may be worthwhile to compare the numerical results of (5″) and of (5‴), i.e. of (5′) with the fudge factors $c = e^{\gamma}/2$ and $c = 1$, respectively, with the actual counts of primes. In the computation we use the value $C = 1{\cdot}378\ldots$ It is easier and more accurate to compute C by the formula $C = 4AB/\pi$, than by its defining, very slowly converging product, because A and B are given by relatively fast converging products, which lead to $A = 0{\cdot}927\ldots$ and $B = 1{\cdot}1680\ldots$ If $c = 1$, the constant becomes $C_1 = 2e^{-\gamma}C = 1{\cdot}546\ldots$ In computing table 1, the values of $N_0(n) = C\sqrt{n}/(\log n)$ and of $N_1(n) = C_1\sqrt{n}/(\log n)$ were computed to two decimal places and those values were used in the computation of the ratios $N(n)/N_0(n)$ and $N(n)/N_1(n)$, where $N(n)$ stands for the actual number of primes represented by $m^2 + 1$, with $m^2 + 1 \leqslant n$. In the listings of the $N_0(n)$ and $N_1(n)$, however, the figures have been rounded off to the nearest integer. For that reason the ratios $N(n)/N_0(n)$ and $N(n)/N_1(n)$ computed with the tabulated figures will, in general, differ from the listed ratios.

In [2] one finds on pp. 43–44 a lengthy argument, why, for numerical comparisons of the present kind, the simple asymptotic formulae, like (5), (5′), etc. should be replaced by others, less simple ones, unless one computers these tabulations for very large values of n (when the difference between the two asymptotic formulae becomes irrelevent). The idea is that some of the terms used in the simple formulae are just the leading terms of asymptotic expansions and that the second (and perhaps even the third) terms of those expansions are by no means negligible with respect to the main term—at least for the moderate values of n, likely to be used. Be that as it may, the tabulation does not suggest at all a convergence of the ratios towards unity, but seems to oscillate in the case of (5″) around the simple constant 4/3. Also in the case of (5‴), the ratio $N(n)/N_1(n)$ seems to stay close to 7/6, rather than converge towards unity. Without any theoretical justification and only for illustrative purposes, we add in table 1 also a column $N_2(n)$, with the entries obtained by using in (5″), instead of C, the constant $C_2 = \frac{4}{3}C$ and $N_3(n)$, where the constant $C_3 = \frac{7}{6}C_1$ has been used. Perhaps the fudge factor c should be $7/6(= 1{\cdot}1666\ldots)$, rather than $e^{\gamma}/2(= 0{\cdot}89\ldots)$, or even $c = 1$?

Table 1. Comparison of formula with empirical results for $y^2 + 1$.

n	$\sqrt{n}/\log n$	$N(n)$	$N_0(n)$	$N(n)/N_0(n)$	$N_1(n)$	$N(n)/N_1(n)$	$N_2(n)$	$N_3(n)$	$N(n)/N_3(n)$
10 000	10·8	19	15	1·28	17	1·14	20	19	0·975
20 000	14·3	26	20	1·32	22	1·18	25	26	1·008
30 000	16·8	30	23	1·30	26	1·16	31	30	0·990
40 000	18·9	33	26	1·27	29	1·13	35	34	0·968
50 000	20·7	36	29	1·26	32	1·125	38	37	0·964
60 000	22·2	40	31	1·31	34	1·17	41	40	0·999
70 000	23·7	44	33	1·35	37	1·20	44	43	1·029
80 000	25·1	46	35	1·33	39	1·19	47	45	1·016
90 000	26·3	47	36	1·30	41	1·16	48	47	0·991
100 000	27·5	50	38	1·32	43	1·18	51	50	1·008

6. The polynomial $f(y) = 1 + y(y+1)/2$

Clearly, $2f(m) = m^2 + m + 2$ can be a prime only for $m = 0$, because, for $m \in \mathbb{Z}$, $f(m)$ is even. We therefore consider $f(y)$, which is integral valued, but does not have integer coefficients. For $m \equiv 1 \pmod 4$ $m \equiv 2 \pmod 4$, $f(m)$ is even; therefore, in order to have $f(m)$ prime, we must take $m \equiv 0$, or $m \equiv 3 \pmod 4$. The number of such integers $m \leqslant x$ is asymptotically equal to $x/2$.

For p odd, $8f(m) = 4m^2 + 4m + 8 = (2m+1)^2 + 7$; hence, $f(m) \equiv 0 \pmod p$ if and only if $u^2 \equiv -7 \pmod p$ has solutions, i.e. precisely when $(-7/p) = 1$. By the quadratic reciprocity law, $(-7/p) = (p/7) = 1$ restricts p to the residue classes 1, 2, or 4 modulo 7. The Legendre symbol $(n/7)$ is the non-principal real character $\chi(n)$ modulo 7. We conclude that in (2)

$$a_p = \begin{cases} 2 & \text{if} \quad p \equiv 1, 2, \quad \text{or} \quad 4 \text{ modulo } 7, \; p \geqslant 3, \\ 1 & \text{if} \quad p = 2, \\ 0 & \text{if} \quad p \equiv 3, 5, \quad \text{or} \quad 6 \text{ modulo } 7. \end{cases}$$

Formula (2) now becomes

$$\tilde{N}(x) \simeq c\frac{x}{2} \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} \left(1 - \frac{2}{p}\right) \tag{6}$$

where $z = x/\sqrt{2}$.

We proceed to compute the product in (6), just as we did with a similar product in § 4.

$$\prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - 2p^{-1}) = \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - p^{-1})^2 \frac{1 - 2p^{-1}}{(1 - p^{-1})^2}$$
$$= \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - p^{-1})^2 \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - (p-1)^{-2}).$$

For $x \to \infty$, also $z \to \infty$ and the second product converges to a constant, say $A = 0{\cdot}983\ldots$ As for the first one, it follows from results in [1] that

$$\prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant x/\sqrt{2}}} (1 - p^{-1})^2 \simeq k_1^2/\log x, \qquad \prod_{\substack{\chi(p)=-1 \\ p \leqslant x/\sqrt{2}}} (1 - p^{-1})^2 \simeq k_{-1}^2/\log x, \tag{7}$$

where

$$k_1^2 = \tfrac{1}{3}4e^{-\gamma} L(1, \chi)^{-1} \prod_{\chi(p)=-1} (1 - p^{-2})^{-1},$$
$$k_{-1}^2 = \tfrac{7}{6}e^{-\gamma} L(1, \chi) \prod_{\chi(p)=-1} (1 - p^{-2}), \tag{8}$$

so that

$$k_{-1}/k_1 = \tfrac{1}{2}L(1, \chi) \prod_{\chi(p)=-1} (1 - p^{-2}). \tag{9}$$

For $\chi(p) = (p/7)$ it may be shown (see [3]) that

$$L(1,\chi) = \frac{\pi}{2\left(-\sin\frac{\pi}{7} + \sin\frac{2\pi}{7} + \sin\frac{3\pi}{7}\right)} = 1{\cdot}18741\ldots$$

Also,

$$\prod_{\chi(p)=-1}(1-p^{-2})^{-1} = 1{\cdot}1900\ldots$$

It follows that $\tilde{N}(x) \simeq (c/2)Ak_1^2 x/\log x$. Next, if $1 + x(x+1)/2 = n$, then $x \simeq \sqrt{2n}$ and, passing from $\tilde{N}(x)$ to $N(n)$, we find

$$N(n) \simeq c\sqrt{2}Ak_1^2\frac{\sqrt{n}}{\log n}. \tag{10}$$

This can still be simplified, as was done for $f(y) = y^2 + 1$. We use once more the simplified writing, when dealing with semiconvergent, or divergent products. We have

$$A = \prod_{\substack{\chi(p)=1\\ p\geqslant 3}}(1-(p-1)^{-2})$$

$$= \prod_{p\geqslant 3}(1-\chi(p)(p-1)^{-1})\left\{\prod_{\substack{\chi(p)=1\\ p\geqslant 3}}(1+(p-1)^{-1})\Big/\prod_{\chi(p)=-1}(1+(p-1)^{-1})\right\}.$$

The first factor converges (conditionally) to a constant $C' = 1{\cdot}970\ldots$ After obvious transformations, the second factor is seen to be equal to

$$\lim_{x\to\infty}\left\{\prod_{\substack{\chi(p)=-1\\ p\leqslant x}}(1-p^{-1})\Big/\prod_{\substack{\chi(p)=1\\ 3\leqslant p\leqslant x}}(1-p^{-1})\right\} = k_{-1}/k_1,$$

where we have used (7). By (9) this ratio equals $\frac{1}{2}L(1,\chi)\prod_{\chi(p)=-1}(1-p^{-2})$, so that

$$A = \tfrac{1}{2}C'L(1,\chi)\prod_{\chi(p)=-1}(1-p^{-2}). \tag{11}$$

The constant in (10) becomes

$$c\frac{\sqrt{2}}{2}C'L(1,\chi)\prod_{\chi(p)=-1}(1-p^{-2})k_1^2 = c\frac{7\sqrt{2}}{3}e^{-\gamma}C',$$

where we made use of (8).

We have completed the proof of

$$N(n) \simeq K\frac{\sqrt{n}}{\log n}, \tag{12}$$

where $K = c(7\sqrt{2}/3)e^{-\gamma}C' \simeq 3{\cdot}65c$.

According to (**), $K = 2C' \simeq 3{\cdot}94\ldots$, the second member of (12), obtained with thi

constant will be denoted by $N_0(n)$. We also consider in (12) the value K_1 of K, obtained with $c = 1$, i.e. $K_1 \simeq 3{\cdot}65$ and denote the corresponding value of $N(n)$ by $N_1(n)$. Finally, we consider the fudge factor $c = e^{\gamma}/2 \simeq 0{\cdot}8905\ldots$, which was valid for $f(y) = y$ and (perhaps) for $f(y) = y^2 + 1$; this leads to $K_2 \simeq 3{\cdot}25$ and we denote the corresponding value of $N(n)$ by $N_2(n)$. If we want to identify $K = K_0$ of (12) with the presumed coefficient $2C'$ of Hardy and Littlewood, in $N_0(n)$, then we have to take

$$c = \frac{3\sqrt{2}}{7}e^{\gamma} = \frac{6\sqrt{2}}{7}(e^{\gamma}/2) \simeq 1{\cdot}212\ldots(e^{\gamma}/2) \simeq 1{\cdot}079\ldots$$

rather than $c = e^{\gamma}/2 \simeq 0{\cdot}8905\ldots$, or $c = 1$.

As in the case of $f(y) = y^2 + 1$, we tabulate the values of (12) (see table 2) obtained with K_0, K_1 and K_2 and compare them with the values $N(n)$, the true number of primes not in excess of n, represented by $f(m)$. As previously, the value $C' \simeq 1{\cdot}970\ldots$ has been computed by use of (11), rather than by the direct evaluation of the defining infinite product, which converges only conditionally and very slowly. The three indicated values of c are too close, to make a significant difference for $n \leqslant 100{,}000$.

We recall that in table 2 the values of the $N_i(n)$ have been rounded off to the nearest integer, while the ratios have been computed with the values furnished by formula (12), with the respective coefficients K_i $(i = 0, 1, 2)$, rounded off to two decimal places.

It appears that the formula that yields the results closest to the true count is obtained by taking the trivial fudge factor $c = 1$ in both cases, $f(y) = y^2 + 1$ and $f(y) = \frac{1}{2}y(y + 1) + 1$.

But one should not be overly impressed by the good fit of the formulae with $c = 1$; as pointed out by Hardy and Littlewood, such considerations can easily be misleading. As long as, e.g. $(\log n)^{-2}$ is not entirely negligible with respect to $(\log n)^{-1}$, one ought to be skeptical. While no amount of computation can decide the validity of any asymptotic formula, more extensive and more accurate computations seem desirable.

At this point it may be worthwhile to recall that in [2; pp. 34–36], Hardy and Littlewood show for the Goldbach problem that, if a formula obtained by sieve methods has the same general structure as one obtained by the circle method, then the constant coefficient can only be the one obtained by the circle method. This reasoning is not immediately applicable to the present situation, but the result of

Table 2. Comparison of formula with empirical results for $\frac{1}{2}y(y + 1) + 1$.

n	$n/\log n$	$N(n)$	$N_0(n)$	$N(n)/N_0(n)$	$N_1(n)$	$N(n)/N_1(n)$	$N_2(n)$	$N(n)/N_2(n)$
10 000	10·86	40	43	0·935	40	1·009	35	1·133
20 000	14·28	50	56	0·889	52	0·959	46	1·077
30 000	16·80	61	66	0·922	61	0·995	55	1·117
40 000	18·87	67	73	0·913	69	0·973	61	1·092
50 000	20·67	73	81	0·896	75	0·968	67	1·087
60 000	22·26	78	88	0·889	81	0·960	72	1·078
70 000	23·72	85	93	0·909	87	0·982	77	1·103
80 000	25·05	91	99	0·922	91	0·995	81	1·118
90 000	26·30	94	104	0·907	96	0·979	85	1·065
100 000	27·47	101	108	0·933	100	1·007	89	1·134

Hardy and Littlewood may have a more general validity than for the Goldbach problem alone. If one could show its validity in the present case, then $N_1(n)$ is the correct asymptotic value for both polynomials here considered, regardless of the better fit of $c = 1$ for "small" values of n.

References

[1] Grosswald E, Some number theoretic products (to appear); see also *Notices of the Am. Math. Soc.* 7 (1986) p. 374
[2] Hardy G H and Littlewood J E, Partitio Numerorum III — *Acta Math.* **44** (1923) 1–70
[3] Landau E, *Die Lehre von der Verteilung der Primzahlen* (New York: Chelsea Pub. Co.) 2nd edn (1953)
[4] Ramanujan's *Notebooks* (Bombay: Tata Institute of Fundamental Research) Photostatic edition in 2 volumes (1959)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 85–109.
© Printed in India.

(GL_n, GL_m)-duality and symmetric plethysm

ROGER HOWE*

The Institute for Advanced Studies, Hebrew University of Jerusalem, Givat Ram 91940, Jerusalem, Israel
Permanent Address: Department of Mathematics, Yale University, Box 2155 Yale Station, New Haven, CT 06520, USA

Abstract. In [7] the author has given an exposition of the theory of invariants of binary forms in terms of a particular version of Classical Invariant Theory. Reflection shows that many aspects of the development apply also to n-ary forms. The purpose of this paper is to make explicit this more general application. The plethysms $S^l(S^2(\mathbb{C}^n))$ are computed quite explicitly for $l = 2$, 3 and 4.

Keywords. (GL_n, GL_m)-duality; plethysm; symmetric plethysm; reciprocity laws; invariants.

1. (GL_n, GL_m)-duality

1.1: By a Young Diagram D we understand a sequence $m_1 \geqslant m_2 \geqslant \ldots$ of decreasing, non-negative integers, only finitely many of which are non-zero. We write $D = D(m_i)$. The sum

$$|D| = \sum_{i>0} m_i \tag{1}$$

is the *size* of D, and the integer k such that $m_k > 0 = m_{k+1}$ is the *depth* of D.

1.2: It is explained in many places (for example [13], [22], [24]) that a certain family of irreducible representations of $GL_n(\mathbb{C})$, the "polynomial" representations, are parametrized by Young Diagrams of depth at most n. Denote by σ_D^n the representation of $GL_n(\mathbb{C})$ parametrized by the Young Diagram D. The determinant character $\det_n$ of $GL_n(\mathbb{C})$ corresponds to the diagram $D(1^n)$, for which $m_i = 1$ for $i \leqslant n$ and $m_i = 0$ for $i > n$. Every representation of $GL_n(\mathbb{C})$ can be obtained from the polynomial ones by tensoring with negative powers of $\det_n$.

1.3: Consider the tensor product $\mathbb{C}^n \otimes \mathbb{C}^m$. We have an action of $GL_n(\mathbb{C})$ on $\mathbb{C}^n \otimes \mathbb{C}^m$ induced by the standard action on $\mathbb{C}^n$. Similarly the action of $GL_m(\mathbb{C})$ on $\mathbb{C}^m$ gives us an action on $\mathbb{C}^n \otimes \mathbb{C}^m$. These actions of GL_n and of GL_m on $\mathbb{C}^n \otimes \mathbb{C}^m$ clearly commute with one another, so we have a joint action of $GL_n \times GL_m$ on $\mathbb{C}^n \otimes \mathbb{C}^m$.

Let $S(\mathbb{C}^n)$ denote the symmetric algebra on $\mathbb{C}^n$. It is standard [18] that the action of GL_n on $\mathbb{C}$ gives rise to an action of GL_n on $S(\mathbb{C}^n)$ by algebra automorphisms. In the situation of the previous paragraph we can consider the restriction of the action

* Partially supported by NSF Grant No. DMS 8506130.

of $GL_{nm}(\mathbb{C})$ on $S(\mathbb{C}^n \otimes \mathbb{C}^m)$ to $GL_n \times GL_m$. For this action, we have an explicit decomposition of $S(\mathbb{C}^n \otimes \mathbb{C}^m)$ into irreducible modules:

$$S(\mathbb{C}^n \otimes \mathbb{C}^m) \simeq \sum_{\text{depth}(D) \leqslant \min(n,m)} \sigma_D^n \otimes \sigma_D^m. \tag{2}$$

This decomposition is well-known, sometimes only implicitly, by various names to various people: [1], [25], [5], [14], [24]. In some sense it is implicit in power series identities going back to Cauchy. From the viewpoint of this author, formula (2) is the simplest case of the duality correspondence for a reductive dual pair [8], [9]. We will refer to the decomposition (2), and the implied correspondence $\sigma_D^n \leftrightarrow \sigma_D^m$ of representations of GL_n and GL_m, as (GL_n, GL_m)-*duality*.

We remark that (GL_n, GL_1)-duality amounts to the very familiar decomposition of $\mathbb{S}(\mathbb{C}^n)$ into its homogeneous components, which are simply the various symmetric powers of $\mathbb{C}^n$:

$$\mathbb{S}(\mathbb{C}^n) \simeq \sum_{l=0}^{\infty} S^l(\mathbb{C}^n). \tag{3}$$

Here $S^l(\mathbb{C}^n)$ indicates the l-th symmetric power of $\mathbb{C}^n$. It is an irreducible module for GL_n.

2. Reciprocity laws for tensor products and for plethysm

From the viewpoint of [8], a key feature of the decomposition (2) is that the irreducible subspaces for $GL_n \times GL_m$ can be characterized either by their behaviour under GL_n or by their behaviour under GL_m. Thus the σ_D^n-isotypic subspace for GL_n acting on $\mathbb{S}(\mathbb{C}^n \otimes \mathbb{C}^m)$ is the irreducible $GL_n \times GL_m$-module $\sigma_D^n \otimes \sigma_D^m$, which is also the σ_D^m-isotypic subspace for the action of GL_m. (For the decomposition (3) this duality consists in characterizing the irreducible GL_n-modules $S^l(\mathbb{C}^n)$ as the "homogeneous symmetric tensors of degree l". The term "homogeneous" refers to the action of the scalar subgroup $GL_1 \subseteq GL_n$: "homogeneous of degree l" means the eigenspace for the character $(\det_1)^l$ of GL_1.) Such a situation gives rise to reciprocity laws. Frobenius Reciprocity in the general theory of group representations is of this nature, as is the "symbolic method" of Classical Invariant Theory. We have noted some reciprocity laws in the context of dual pairs in [7] and [10]. Here we will describe some reciprocity laws relevant to the problems of decomposing tensor products and plethysm.

2.1: We first extend Remark 4.3.3.10 of [7], and give the proof. Fix n, and consider Young Diagrams D_i, $1 \leqslant i \leqslant l$, of depths k_i, with $k_i \leqslant n$. Consider the tensor product

$$\prod(D_1, D_2, \ldots, D_l) = \sigma_{D_1}^n \otimes \sigma_{D_2}^n \otimes \cdots \otimes \sigma_{D_l}^n. \tag{4}$$

We want to decompose $\prod(D_i)$ into irreducible representations. In particular if σ_E^n is another irreducible representation of GL_n, we would like to know the multiplicity

$$\dim \text{Hom}\,(\sigma_E^n, \prod(D_1, \ldots, D_l))^{GL_n} = \mu(E; D_1, \ldots, D_l) \tag{5}$$

with which σ_E^n occurs in $\prod(D_i)$.

Choose integers m_i with $m_i \geqslant k_i$. Then the $(GL_n \times GL_{m_i})$-module $\sigma^n_{D_i} \otimes \sigma^{m_i}_{D_i}$ is the $\sigma^n_{D_i}$-isotypic component of the GL_n action on $S(\mathbb{C}^n \otimes \mathbb{C}^{m_i})$, and is likewise the $\sigma^{m_i}_{D_i}$-isotypic component for the action of GL_{m_i}. Thus the tensor product

$$\begin{aligned}&(\sigma^n_{D_1} \otimes \sigma^{m_1}_{D_1}) \otimes (\sigma^n_{D_2} \otimes \sigma^{m_2}_{D_2}) \otimes \cdots \otimes (\sigma^n_{D_l} \otimes \sigma^n_{D_l} \otimes \sigma^{m_l}_{D_l}) \\ &\quad \simeq (\sigma^n_{D_1} \otimes \sigma^n_{D_2} \otimes \cdots \otimes \sigma^n_{D_l}) \otimes (\sigma^{m_1}_{D_1} \otimes \cdots \otimes \sigma^{m_l}_{D_l}) \\ &\quad = \prod (D_1, \ldots, D_l) \otimes \left(\bigotimes_i \sigma^{m_i}_{D_i} \right) \end{aligned} \tag{6}$$

is characterizable as the $\left(\bigotimes_i \sigma^{m_i}_{D_i} \right)$-isotypic component for the action of

$$\prod_i GL_{m_i} \quad \text{on} \quad \bigotimes_i S(\mathbb{C}^n \otimes \mathbb{C}^{m_i}).$$

On the other hand, the obvious identification

$$\sum_i \mathbb{C}^{m_i} \simeq \mathbb{C}^m, \quad m = \sum_i m_i, \tag{7}$$

obtained by stacking the m_i-tuples of the various $\mathbb{C}^{m_i}$ consecutively in one long column of length m, yields a natural isomorphism

$$\bigotimes_i \mathbb{S}(\mathbb{C}^n \otimes \mathbb{C}^{m_i}) \simeq \mathbb{S}(\mathbb{C}^n \otimes \mathbb{C}^m). \tag{8}$$

Further the identification (7) yields an embedding

$$\prod GL_{m_i} \subsetneq GL_m. \tag{9}$$

Here $\prod_i GL_{m_i}$ is identified to the "block diagonal" subgroup of GL_m consisting of $g \in GL_m$ which preserve the decomposition (7) of $\mathbb{C}^m$. These identifications allow us to describe $\prod (D_i) \otimes \left(\bigotimes_i \sigma^{m_i}_{D_i} \right)$ as the $\left(\bigotimes_i \sigma^{m_i}_{D_i} \right)$-isotypic subspace of $\mathbb{S}(\mathbb{C}^n \otimes \mathbb{C}^m)$ under the action of the subgroup $\prod_i GL_{m_i}$ of GL_m.

Returning to consideration of the GL_n action, we observe that $\prod (D_i) \otimes \left(\bigotimes_i \sigma^{m_i}_{D_i} \right)$ is also of course invariant under GL_n. We consider its decomposition into irreducible GL_n-modules. We can describe this as

$$\begin{aligned}\prod (D_i) \otimes \left(\bigotimes_i \sigma^{m_i}_{D_i} \right) &\simeq \sum_E \mu(E; D_1, \ldots, D_l) \sigma^n_E \otimes \left(\bigotimes_i \sigma^{m_i}_{D_i} \right) \\ &\simeq \sum_E \sigma^n_E \otimes \left(\mu(E; D_1, \ldots, D_l) \bigotimes_i \sigma^{m_i}_{D_i} \right) \end{aligned} \tag{10}$$

Since the σ^n_E-isotypic subspace of $\mathbb{S}(\mathbb{C}^n \otimes \mathbb{C}^m)$ is equally the σ^m_E-isotypic subspace, we

see that the summand

$$\sigma_E^n \otimes \left(\mu(E; D_1, \ldots, D_l) \bigotimes_i \sigma_{D_i}^{m_i} \right)$$

is describable as the $\left(\bigotimes_i \sigma_{D_i}^{m_i} \right)$-isotypic subspace for the restriction of the representation σ_E^m to $\prod_i GL_{m_i}$. In particular we have the following reciprocity law.

PROPOSITION

The multiplicity

$$dim\, Hom\left(\sigma_E^n, \bigotimes_i \sigma_{D_i}^n \right)^{GL_n}$$

of the irreducible representation σ_E^n of GL_n in the l-fold tensor product of representations $\sigma_{D_i}^n$ is equal to the multiplicity

$$dim\, Hom\left(\sigma_E^m, \bigotimes_i \sigma_{D_i}^{m_i} \right)^H$$

of the representation

$$\bigotimes_i \sigma_{D_i}^{m_i} \quad of \quad H = \prod_i GL_{m_i}$$

in the restriction to the subgroup $\prod_i GL_{m_i}$ of the irreducible representation σ_E^m of GL_m.

2.2: *Remarks:*

(a) More or less the observation of Proposition 2.1 has also been made by Klink and Ton-That [16]. As they point out, the (GL_n, GL_m)-duality can be used to get much finer information than just multiplicities.

(b) When $l = 2$, the multiplicities $\mu(E; D_1, D_2)$ are known as Littlewood–Richardson coefficients and have been described combinatorially [21], [13]. If one knows how to describe two-fold tensor products, then l-fold tensor products may be decomposed by an obvious recursive procedure. However, the all-in-one description of multiplicities afforded by Proposition 2.1 may sometimes be advantageous. We note that a combinatorial description of the restriction of σ_E^m to $\prod GL_{m_i}$ is given in [19].

(c) We are principally interested here in the case when each $\sigma_{D_i}^n$ is simply a symmetric power $S^{p_i}(\mathbb{C}^n)$. For this case the reciprocity of §2.1 takes a particularly simple form, which we will make explicit.

Let $A = A_n \subseteq GL_n$ be the standard maximal torus:

$$A = \left\{ \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix} = t(a_1, a_2, \ldots, a_n), a_i \in \mathbb{C}^* \right\}. \tag{11}$$

The map $t(a_1,\dots,a_n)\to(a_1,a_2,\dots,a_n)$ sending an element of A to the n-tuple of its diagonal entries defines an isomorphism of groups between A and $(GL_1)^n$. Since A is abelian, its irreducible rational representations are all one-dimensional, and are identifiable with rational characters. These have the form

$$\psi_p: t(a_1,\dots,a_n)\to a_1^{p_1}a_2^{p_2}\cdots a_n^{p_n}, \tag{12}$$

where $p=(p_1,p_2,\dots,p_n)$ is an n-tuple of integers.

If, in the discussion of § 2.1 we take each $\sigma^n_{D_i}$ to be a symmetric power $S^{p_i}(\mathbb{C}^n)$, then we may take each m_i to be 1. Then we will have

$$m=\sum_{i=1}^{l} m_i = l, \quad \text{and} \quad \prod_i GL_{m_i} = A_l,$$

the standard maximal torus in GL_l. Thus Proposition 2.1 reduces to the following statement.

13. COROLLARY

The multiplicity of a representation σ^n_E of GL_n in a tensor product $\bigotimes_{i=1}^{l} S^{p_i}(\mathbb{C}^n)$ is equal to the multiplicity of the character ψ_p, $p=(p_1,\dots,p_l)$ of the maximal torus $A_l\subseteq GL_l$ in the representation σ^l_E of GL_l.

(d) Theorem 7.6F, page 207, in [24], properly read, is essentially equivalent to Corollary 13. The Corollary may also be gleaned from [20], formula (6.4;6), page 104, which is attributed to Kostka.

(e) The multiplicities of characters of A_l in representations of GL_l is about as standard technology as exists in the subject of representation theory. In particular, one has the formulas of Freudenthal and of Kostant [12] for such multiplicities. Also there are combinatorial descriptions (Kostka, Gelfand–Zetlin [25], [13]) of bases for the A_l-eigenspaces. In this sense Corollary 13 is a solution to the problem of decomposing $\bigotimes_{i=1}^{l} S^{p_i}(\mathbb{C}^n)$. On the other hand, the actual computation of these multiplicities is not entirely unproblematic. See § 3.5 for some examples.

2.3: We now discuss how to adapt Proposition 2.1 to describe plethysm. First let us recall what plethysm is.

The basis for plethysm is Schur Duality [24], [25], [21], which we will recall briefly. Schur Duality is the description of the decomposition into irreducible representations for GL_n of the l-fold tensor power $(\mathbb{C}^n)^{\otimes l}=T^l(\mathbb{C}^n)$ of $\mathbb{C}^n$. We observe that there is an action of the symmetric group S_l on $T^l(\mathbb{C}^n)$, by permutation of the factors in the tensor product:

$$\pi(v_1\otimes v_2\otimes\cdots\otimes v_l)=v_{\pi^{-1}(1)}\otimes v_{\pi^{-1}(2)}\otimes\cdots\otimes v_{\pi^{-1}(l)} \quad v_i\in\mathbb{C}^n, \quad \pi\in S_l. \tag{14}$$

This action of S_l obviously commutes with GL_n, so we have a joint action of $GL_n\times S_l$ on $T^l(\mathbb{C}^n)$. Schur Duality says that as $GL_n\times S_l$ module we have

$$T^l(\mathbb{C}^n)\simeq \sum_{\substack{|D|=l\\ \operatorname{depth}(D)\leqslant n}} \sigma^n_D\otimes J_D, \tag{15}$$

where $D \to J_D$ is a certain parametrization of the irreducible representations of S_l by the Young Diagrams of size l.

It follows from decomposition (15) that the irreducible polynomial representations of GL_n can be distinguished by how their realizations in $T^l(\mathbb{C}^n)$ transform under S_l. In other words, irreducible polynomial representations of GL_n can be described as tensors having certain symmetry properties—as symmetry classes of tensors in short. Furthermore, this description depends only on the Young Diagram, not on n, so in fact the irreducible representations of GL_n can be regarded as arising by the performance of certain functorial constructions on $\mathbb{C}^n$. These functorial constructions are again labelled by Young Diagrams. In honour of this elevation of the representations σ_D^n to the status of functors, we will denote them by $S^D(\mathbb{C}^n)$. More precisely, we will denote by $S^D(\mathbb{C}^n)$ a space of tensors of the symmetry class defined by D. It will be understood to carry a canonical structure of GL_n-module, giving a realization of σ_D^n. If depth (D) exceeds n, then $S^D(\mathbb{C}^n) = \{0\}$.

In this setting, the problem of plethysm may be stated: compute the composition of two of these functors. That is we want to find the irreducible decomposition of

$$(S^E \circ S^D)(\mathbb{C}^n) = S^E(S^D(\mathbb{C}^n)) \tag{16}$$

for two Young Diagrams D, E.

2.4: We will develop a reciprocity law for describing the plethysm (16). We assume that $n \geqslant \text{depth}(D)$. Choose $m \geqslant \text{depth}\ (D)$. Then $S^D(\mathbb{C}^n) \otimes S^D(\mathbb{C}^m)$ is a summand of $S(\mathbb{C}^n \otimes \mathbb{C}^m)$. Let l be the size of the Young Diagram E. Then $T^l(S^D(\mathbb{C}^n) \otimes S^D(\mathbb{C}^m)) \simeq T^l(S^D(\mathbb{C}^n)) \otimes T^l(S^D(\mathbb{C}^m))$ is a subspace of $T^l(S(\mathbb{C}^n \otimes \mathbb{C}^m)) \simeq S((\mathbb{C}^n \otimes \mathbb{C}^m)^l) \simeq S(\mathbb{C}^n \otimes (\mathbb{C}^m)^l)$. Furthermore $T^l(S^D(\mathbb{C}^n)) \otimes T^l(S^D(\mathbb{C}^m))$ is characterized as the $(\sigma_D^m)^{\otimes l}$-isotypic component for the action of $(GL_m)^l \subseteq GL_{ml}$ on $S(\mathbb{C}^n \otimes (\mathbb{C}^m)^l)$.

The symmetric group S_l acts on $(\mathbb{C}^m)^l$ by permuting the copies of $\mathbb{C}^m$. This action normalizes $(GL_m)^l$ inside GL_{ml}. It is easy to check that, in fact, the normalizer of $(GL_m)^l$ inside GL_{ml} is precisely the semidirect product

$$S_l \circledS (GL_m)^l \quad .$$

The representation $(\sigma_D^m)^{\otimes l}$ of $(GL_m)^l$ is stable under conjugation by S_l. There is a unique extension of $(\sigma_D^m)^{\otimes l}$ to a representation of $S_l \circledS (GL_m)^l$ such that S_l leaves fixed all tensors of the form $y^{\otimes l} = y \otimes y \otimes \cdots \otimes y$ (l-factors), $y \in S^D(\mathbb{C}^m)$. Denote this representation by $(\sigma_D^m)_{(l)}$. From the general theory of group representations (Clifford Theory [2]) we know that every representation of $S_l \circledS (GL_m)^l$ which restricts to a multiple of $(\sigma_D^m)^{\otimes l}$ on $(GL_m)^l$ has the form $(\sigma_D^n)_{(l)} \otimes J_E$ where E is a Young Diagram of size l, and J_E is the corresponding representation of S_l. Let us write

$$(\sigma_D^m)_{(l)} \otimes J_E = \sigma_{D,E}^m. \tag{17}$$

Return now to consideration of the space $T^l(S^D(\mathbb{C}^n) \otimes S^D(\mathbb{C}^m))$. Fix a vector y in $S^D(\mathbb{C}^m)$. Then the subspace $T^l(S^D(\mathbb{C}^n)) \otimes (y^{\otimes l})$ of $T^l(S^D(\mathbb{C}^n) \otimes S^D(\mathbb{C}^m))$ is invariant under GL_n and under S_l. It is clear that the action of GL_n on $T^l(S^D(\mathbb{C}^n)) \otimes (y^{\otimes l})$ is simply $(\sigma_D^n)^{\otimes l}$. (This is an inner tensor product: a representation of GL_n, not $(GL_n)^l$). We have not distinguished notationally between this inner tensor product and the outer tensor product $(\sigma_D^m)^{\otimes l}$, which was a representation of the l-fold product $(GL_m)^l$, rather than

its diagonal subgroup. We hope which tensor product is meant will be clear from context.) It is also clear that the action of S_l on $T^l(S^D(\mathbb{C}^n))\otimes(y^{\otimes l})$ is equivalent to the standard action of S_l on $T^l(S^D(\mathbb{C}^n))$. Thus we have a decomposition

$$T^l(S^D(\mathbb{C}^n))\otimes(y^{\otimes l})\simeq\sum_{|E|=l}S^E(S^D(\mathbb{C}^n))\otimes J_E. \tag{18}$$

Combining this with our description (17) of the representations of $S_l\times(GL_m)^l$, we find a decomposition

$$T^l(S^D(\mathbb{C}^n))\otimes S^D(\mathbb{C}^n)\simeq\sum_{|E|=l}S^E(S^D(\mathbb{C}^n))\otimes\sigma^m_{D,E} \tag{19}$$

of $GL_n\times(S_l\circledS(GL_m)^l)$-modules. In particular, since (18) is an isotypic decomposition for the action of S_l, we see that

$$S^E(S^D(\mathbb{C}^n))\otimes\sigma^m_{D,E}$$

is the $\sigma^m_{D,E}$-isotypic component of $S(\mathbb{C}^n\otimes(\mathbb{C}^m)^l)$ under the action of $S_l\times((GL_m)^l)$. Combining this with the reasoning of § 2.1, we arrive at the following conclusion.

PROPOSITION

Given Young Diagrams D, E and F, and an integer m, at least as large as depth (D), the multiplicity

$$dim\,Hom(S^F(\mathbb{C}^n), S^E(S^D(\mathbb{C}^n)))^{GL_n}$$

with which $S^F(\mathbb{C}^n)$ occurs in $S^E(S^D(\mathbb{C}^n))$ is equal to the multiplicity

$$dim\,Hom(\sigma^{ml}_F, \sigma^m_{D,E})^H$$

with which the representation $\sigma^m_{D,E}$ of $H=S_l\circledS(GL_m)^l$ occurs in the restriction to $S_l\times(GL_m)^l$ of the representation σ^{ml}_F of GL_{ml}. Here $l=|E|$. The multiplicity will be zero unless $|F|=l|D|$.

2.5: We are especially interested in the case of Proposition 2.4 when $D=\{p\}$ and $E=\{l\}$ have depth 1, i.e. the case of $S^l(S^p(\mathbb{C}^n))$. Here we can choose $m=1$. Then, as in §2.2, Remark (c), we have $(GL_1)^l\simeq A_l$, the standard maximal torus in GL_l. Further the representation $(\sigma^1_{\{p\}})^{\otimes l}$ of A_l is simply the character $\psi_{(p,p,\ldots,p)}$ in the notation of (12). It is just the restriction to A_l of the character $(\det_l)^p$ of GL_l. Further the group S_l is simply the Weyl group of GL_l, and the representation $(\sigma^1_{\{p\}})_{(l)}$ is again simply a character of $S_l\circledS A_l$. (Note, however, it is *not* the restriction of $(\det_l)^p$, unless p is even.) Further $(\sigma^1_{\{p\}})_{(l)}$ is the p-th power of the character $(\sigma^1_{\{1\}})_{(l)}$. Let us denote this character by χ_l. Then

$$(\sigma^1_{\{p\}})_{(l)}=\chi_l^p \quad \text{and} \tag{20}$$

we can enunciate the specialization of Proposition 2.4 to the case at hand as follows.

The multiplicity of

$$\sigma_D^n \quad in \quad S^l(S^p(\mathbb{C}^n)) \tag{21}$$

is equal to the multiplicity with which the character χ_l^p of $S_l \circledS A_l$ occurs in the restriction of σ_D^l to $S_l \circledS A_l$.

Remarks:

(a) The plethysm $S^l(S^p(\mathbb{C}^n))$ is especially relevant to the classical problem of invariants of n-ary forms. Indeed, up to questions of contragredience, which in this situation is mostly a matter of taste, the problem of describing the invariants of a polynomial of degree p in n variables is to find the SL_n invariants in the symmetric algebra

$$S(S^p(\mathbb{C}^n)) = \sum_{l \geq 0} S^l(S^p(\mathbb{C}^n)).$$

And the problem of describing the covariants is to find the full decomposition of $S(S^p(\mathbb{C}^n))$. This amounts to computing the plethysms $S^l(S^p(\mathbb{C}^n))$ for all l.

(b) As people learned in the 19th century, the problem of computing $S^l(S^p(\mathbb{C}^n))$ is very difficult—even if one only takes $p = 2$, and only looks for invariants. To ease their task, the 19th century invariant theorists observed that $S(S^p(\mathbb{C}^n))^{SL_n}$ is an algebra (the algebra of invariants of the n-ary p-ic) and hoped to find a finite set of generators for this algebra. Hilbert made history by showing that this was in principle always possible. But it has proved daunting to do this in concrete instances, and has been accomplished only in a short list of cases, even when $n = 2$.

The reciprocity law (21) introduces another algebra structure on the spaces $S^l(S^p(\mathbb{C}))$. More precisely, the specialization of the decomposition (19) to the case of $S^l(S^p(\mathbb{C}^n))$ shows that

$$S^l(S^p(\mathbb{C}^n)) \simeq S(\mathbb{C}^n \otimes \mathbb{C}^l)^{\chi_l^p} \tag{22}$$

is the χ_l^p-isotypic component of $S(\mathbb{C}^n \otimes \mathbb{C}^l)$ under the action of $S_l \circledS A_l$. Since χ_l is a one-dimensional representation of $S_l \circledS A_l$, we see that the direct sum

$$\sum_{p \geq 0} S(\mathbb{C}^n \otimes \mathbb{C}^l)^{\chi_l^p} \simeq \sum_{p \geq 0} S^l(S^p(\mathbb{C}^n)) \tag{23}$$

is a subalgebra of $S(\mathbb{C}^n \otimes \mathbb{C}^l)$. As is explained in [7], the implicit use of this and closely related algebras was an important technique in 19th century work on binary invariants.

(c) The two algebra structures described in the previous remark are related. Precisely, we observe that

$$S^l(\mathbb{C}^n) = S^l(S^l(\mathbb{C})) \simeq S(\mathbb{C}^n \otimes \mathbb{C}^l)^{\chi_l} \tag{24}$$

sits inside the algebra (23) as the homogeneous component of smallest positive degree. From the universal property of the symmetric algebra [18], we deduce an algebra

homomorphism

$$\text{(a)} \qquad \alpha: \mathbb{S}(S^l(\mathbb{C}^n)) \to \sum_{p \geq 0} \mathbb{S}(\mathbb{C}^n \otimes \mathbb{C}^l)^{\chi^p}, \tag{25a}$$

which consists of maps between each pair of homogeneous components

$$\text{(b)} \qquad \alpha: S^p(S^l(\mathbb{C}^n)) \to S^l(S^p(\mathbb{C}^n)). \tag{25b}$$

When $n > 2$, it is not hard to see that the maps (25b) are all isomorphisms. This gives a very precise version of Hermite Reciprocity [7].

For $n > 2$, the maps (25b) cannot always be isomorphisms. In a conversation with the author, A. Garsia remarked that numerical evidence suggests that there should exist a GL_n-module embedding of $S^p(S^l(\mathbb{C}^n))$ into $S^l(S^p(\mathbb{C}^n))$ when $l \geq p$. This conjecture was also made in [4]. Thus perhaps it is reasonable to expect that the maps (25b) should be injective if $p \leq l$, and surjective if $l \leq p$.

3. Computational considerations and examples

There exist algorithms for computing plethysms (see [1] and the references therein). However, it is this author's understanding that the problem is still considered a difficult one, in that the necessary computations increase rapidly with the size of the partitions involved in the plethysm. This is probably an intrinsic feature of the problem. However, it is conceivable that the reciprocity laws of §2 could be useful in some computations. In this section we will discuss some procedures based on the reciprocity laws for calculating multiplicities in symmetric plethysms, and give some examples. In particular, we give the decomposition of $S^l(S^p(\mathbb{C}^n))$ for $l = 2, 3, 4$. The cases $l = 2$, 3 are in [1], who attribute them to [23]. The case $l = 4$ is treated in [3]. Our formulas are more explicit.

3.1: Although there is a good deal of literature describing weight spaces for representations of semisimple Lie groups (dimensions, and nice bases), this literature is not well-adapted for computation of Weyl group actions. In particular, the standard bases (given in terms of standard tableaux, or Gelfand–Zetlin data) do not transform particularly nicely under the Weyl group. Nevertheless standard technology can be brought to bear on the computation of $S^l \circ S^p$. We will discuss application of the Schur–Weyl Character Formula, the Branching Laws, and Schur Orthogonality.

Consider a representation σ^n_D of GL_n. According to corollary (13) the multiplicity of σ^n_D in $T^l(S^p(\mathbb{C}^n))$ is equal to the dimension of the A_l eigenspace for the character $(\det_l)^p$ of A_l in the representation σ^l_D of GL_l. Since this eigenspace can also be characterized as the fixed points for the subgroup

$$A^1_l = A_l \bigcap SL_l$$

we will refer to it as the "zero weight space".

The symmetric group S_l (the Weyl group of GL_l) acts on the zero weight space of σ^n_D. Corollary (21) says that the multiplicity of σ^n_D in $S^l(S^p(\mathbb{C}^n))$ is equal to the dimension of the space of S_l-invariant vectors in the zero weight space.

One way to compute the dimension of the S_l invariants in the zero weight space is by computing the character of the action of S_l on the zero weight space, then averaging over S_l. Thus denote by η_D^l the action of S_l on the zero weight space of σ_D^l. Then we have

$$\dim \mathrm{Hom}\,(\sigma_D^n, S^l(S^D(\mathbb{C}^n)))^{GL_n} = \left(\sum_{x \in S_l} \mathrm{trace}\, \eta_D^l(x)\right) \Big/ l! \tag{26}$$

The next few subsections discuss the details of implementing formula (26).

3.2: To compute trace $\eta_D^l(x)$, we can use the Schur–Weyl Character Formula and Branching Laws. To begin, let x be a cycle of length l. If ψ_b, $b = (b_1, b_2, \ldots, b_l)$, is a character of A_l, then conjugation by x transforms ψ_b to $\psi_{x(b)}$, where

$$x(b) = (b_{x^{-1}(1)}, b_{x^{-1}(2)}, \ldots, b_{x^{-1}(l)}).$$

The action of $\sigma_D^l(x)$ will send the ψ_b eigenspace for A_l in $S^D(\mathbb{C}^n)$ to the $\psi_{x^{-1}(b)}$ eigenspace. Since x acts transitively on $\{1, 2, \ldots, l\}$, the only b for which the ψ_b eigenspace can be invariant under x is the b such that $b_i = b_j$ for all i, j, i.e. the zero weight space. Thus only the zero weight space can contribute to the trace of $\sigma_D^l(x)$ acting on $S^D(\mathbb{C}^l)$.

27. Lemma: Let $x \in S_l$ be an l-cycle. Then

$$\mathrm{trace}\, \eta_D^l(x) = \mathrm{trace}\, \sigma_D^l(x).$$

To compute this we use the Weyl–Schur Formula ([24]). This formula expresses trace $\sigma_D^l(x)$ as the quotient of two determinants:

$$\mathrm{trace}\, \sigma_D(x) = \frac{\det \begin{bmatrix} \xi_1^{m_1+l-1} & \cdots & \xi_1^{m_l} \\ \vdots & & \\ \xi_l^{m_1+l-1} & \cdots & \xi_l^{m_l} \end{bmatrix}}{\det \begin{bmatrix} \xi_1^{l-1} & \xi_1^{l-2} & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ \xi_l^{l-1} & \xi_l^{l-2} & \cdots & 1 \end{bmatrix}} \tag{28}$$

Here $D = (m_1, m_2, \ldots, m_l)$, and the ξ_i are the eigenvalues of x. For our l-cycle x, the eigenvalues are just ξ^j, $0 \leqslant j < l$, where $\xi = \exp(2\pi i/l)$ is a primitive l-th root of unity.

The determinant in the denominator in (28) is just the van der Mond determinant of $\xi_1, \ldots, \xi_l$. Because of the special form of the eigenvalues of our x, we see by inspecting the columns of the determinant in the numerator of (28) that it also is a van der Mond determinant, of $\xi^{m_1+l-1}, \xi^{m_2+l-2}, \ldots, \xi^{m_l}$. Combining this observation with (28) and (27), we arrive at the following conclusion (29). For an l-cycle x in S_l, we have

$$\mathrm{trace}\, \eta_D^l(x) = \begin{cases} 0 & \text{if } (m_1+l-1, m_2+l-2, \ldots, m_1) \text{ is not a permutation} \\ & \text{of } (l-1, l-2, \ldots, 0) \text{ (modulo } l\text{)}, \\ 1 & \text{if } (m_1+l-1, \ldots, m_1) \text{ is an even permutation} \\ & \text{of } (l-1, l-2, \ldots, 0) \text{ (modulo } l\text{)}, \\ -1 & \text{if } (m_1+l-1, \ldots, m_1) \text{ is an odd permutation} \\ & \text{of } (l-1, l-2, \ldots, 0) \text{ (modulo } l\text{)}. \end{cases} \tag{29}$$

3.3: Formula (29) allows one to reduce the computation of trace $\eta^l_D(x)$ to computing the restriction of σ^l_D to a "block diagonal" subgroup $\prod_{i=1}^{k} GL_{l_i}, \sum l_i = l$ of the sort described in (7) and (9). For consider an element $y \in S_l$. Up to conjugation in S_l, we may assume each cycle of y consists of consecutive integers. Let the cycle lengths of y be $l_1, l_2, \ldots, l_k$. Then y belongs to $\prod_{i=1}^{k} GL_{l_i}$, and if we factor y:

$$y = \prod_i y_i \quad y_i \in GL_{l_i} \tag{30}$$

into its pieces belonging to the various GL_{l_i}, we see each y_i is an l_i-cycle in GL_{l_i}, so the argument of § 3.2 applies to y_i.

Now suppose we know how σ^l_D decomposes on restriction to $\prod_i GL_{l_i}$:

$$\sigma^l_D \Big| \prod GL_{l_i} \simeq \sum_{E_i} m(D; E_1, E_2, \ldots, E_k) \left(\bigotimes_i \sigma^{l_i}_{E_i} \right). \tag{31}$$

Since each irreducible component $\bigotimes_i \sigma^{l_i}_{E_i}$ of the restriction is invariant under A_l (since $A_l \subseteq \prod_i GL_{l_i}$), the zero weight space of σ^l_D will be the direct sum of its intersection with the $\bigotimes_i \sigma^{l_i}_{E_i}$. Furthermore, we can determine whether or not this intersection is non-zero or not simply by looking at the $\sigma^{l_i}_{E_i}$. For if the intersection is non-zero, it will equal the tensor product of the zero weight spaces of the $\sigma^{l_i}_{E_i}$. Thus the question simply is: do the $\sigma^{l_i}_{E_i}$ have zero weight spaces, and, if so, does the character of $A_l \cap GL_{l_i}$ acting on the zero weight space of $\sigma^{l_i}_{E_i}$ coincide with $(\det_{l_i})^p$? This last question is the same as saying: does $A_l \cap GL_{l_i}$ acting via $\sigma^{l_i}_{E_i}$ have $(\det_{l_i})^p$ as an eigencharacter? The answer is yes precisely when $|E_i| = pl_i$. Combining this observation with formula (29) gives the recipe

$$\text{(a)} \qquad \operatorname{trace} \eta^l_D(y) = \sum_{|E_i| = pl_i} m(D; E_1, E_2, \ldots, E_k) \left(\prod_i \epsilon(E_i) \right), \tag{32a}$$

where $\epsilon(E_i)$ is the number defined by the right hand side of formula (29)

$$\text{(b)} \qquad \epsilon(E) = \begin{cases} 1 & \text{according as } (q_1 + m - 1, q_2 + m - 2, \ldots, q_m) \text{ is an} \\ -1 & \text{even permutation, an odd permutation, or not} \\ 0 & \text{a permutation of } (m-1), m-2, \ldots, 0. \end{cases} \tag{32b}$$

Here E is a Young Diagram of depth m with row lengths $(q_1, q_2, \ldots, q_m)$.

3.4: If we do not feel so confident about our ability to write down the decomposition (31) for a general "block diagonal" subgroup $\prod_i GL_{l_i}$, but feel reasonably good about the case of two blocks $GL_{l_1} \times GL_{l_2}$ (the Levi component of a *maximal* parabolic subgroup) then we can compute $\eta^l_D(y)$ by recursion. Suppose we know that

$$\sigma^l_D = \sum_{E_1, E_2} m(D; E_1, E_2) \sigma^{l_1}_{E_1} \otimes \sigma^{l_2}_{E_2} \tag{33}$$

for each l_1, l_2 with $l_1 + l_2 = l$. As in § 3.3, we can argue that the zero weight space is a direct sum of its intersections with the irreducible components $\sigma_{E_1}^{l_1} \otimes \sigma_{E_2}^{l_2}$, and that this intersection is non-zero if and only if $|E_i| = pl_i$. Suppose y in S_l has a decomposition

$$y = y_1 y_2 \quad y_i \in GL_{l_i}. \tag{34}$$

(Here we do not specify that the y_i's should be l_i-cycles. They can be arbitrary elements of S_{l_i}. The only important point here is that y should stabilize the subsets $\{1, 2, \ldots, l_1\}$ and $\{l_1 + 1, l_1 + 2, \ldots, l\}$ of $\{1, 2, \ldots, l\}$.) Reasoning similar to that of § 3.3 tells us

$$\eta_D^l(y) = \sum_{|E_i| = pl_i} m(D; E_1, E_2) \eta_{E_1}^{l_1}(y_1) \eta_{E_2}^{l_2}(y_2). \tag{35}$$

Since, as noted in Remark 2.2(b), the coefficients $m(D; E_1, E_2)$ are Littlewood–Richardson coefficients, formula (35) reduces computation of symmetric plethysms to the decomposition of (general) tensor products.

3.5: Here are some calculations for $l = 2, 3, 4$ based on the procedures outlined above.

Notation: We denote by c_k, $k > 1$, a permutation in S_l consisting of one cycle of length k and $l - k$ fixed points. A permutation with *disjoint* cycles of lengths $k_i, k_i > 1$, will be denoted by $c_{k_1} c_{k_2} c_{k_3} \ldots$. This notation is satisfactory since we are only dealing with properties of conjugacy classes of permutations. The identity element of S_l will just be denoted by 1.

Before beginning we note that, although formula (29) effectively summarizes the combinatorial content of formula (28), there is also the well-known formula for the value of the van der Mond determinant, and this formula can be more convenient for computational purposes. Therefore we record the formula here. Recall $\xi = \exp[(2\pi i)/l]$.

$$\begin{aligned} \operatorname{trace} \eta_D^l(c_l) &= \frac{\prod_{0 \leqslant i < j < l} (\xi^{m_i + l - i} - \xi^{m_j + l - j})}{\prod_{0 \leqslant i < j < l} (\xi^j - \xi^i)} \\ &= \frac{\prod_{0 \leqslant i < j < l} \xi^{(m_i - m_j - i + j)/2} (\xi^{(\mu_{ij})/2} - \xi^{-(\mu_{ij})/2})}{\prod_{0 \leqslant i < j < l} \xi^{(i+j)/2} (\xi^{(j-i)/2} - \xi^{-(j-i)/2})} \\ &= \prod_{0 \leqslant i < j < l} \frac{(\xi^{(\mu_{ij})/2} - \xi^{-(\mu_{ij})/2})}{(\xi^{(j-i)/2} - \xi^{(i-j)/2})}, \end{aligned} \tag{36a}$$

where

$$\mu_{ij} = \sum_{a=i}^{j-1} \mu_a, \quad \mu_i = m_i - m_{i+1+1}. \tag{36b}$$

Now we consider computing the plethysms $S^l(S^p(\mathbb{C}^n))$ for $l = 2, 3, 4$.

$l = 2$: Consider a depth 2 Young Diagram $D = (b_1, b_2)$. In order for σ_D^n to occur in $S^2(S^p(\mathbb{C}^n))$ we need $|D| = b_1 + b_2 = 2p$. We assume this holds. Then the dimension of the zero weight space, and all non-trivial A_2 eigenspaces, of σ_D^2 is well-known to be 1.

The only non-identity element of S_2 is c_2. From formula (36) we can compute

$$\text{trace}\,\eta_D^2(c_2) = (-1)^{b_2} = (-1)^{b_1}. \tag{38}$$

Thus formula (26) specializes to

$$\dim \text{Hom}(\sigma_D^n, S^2(S^p(\mathbb{C}^n))) = \frac{1+(-1)^{b_2}}{2} \tag{39a}$$

$$D = (b_1, b_2), \quad b_1 + b_2 = 2p$$

or

$$\dim \text{Hom}(\sigma_D^n, S^2(S^p(\mathbb{C}^n))) = \begin{cases} 1 & \text{if } b_2 \text{ is even} \\ 0 & \text{if } b_2 \text{ is odd.} \end{cases} \tag{39b}$$

$l = 3$: Consider a depth 3 Young Diagram $D = (b_1, b_2, b_3)$, $a_1 \geqslant a_2 \geqslant a_3 \geqslant 0$. We assume $b_1 + b_2 + b_3 = 3p$, so that σ_D^n has some possibility of occurring in $S^3(S^p(\mathbb{C}^n))$. There are 3 conjugacy classes in S_3, viz. 1, c_2, and c_3. The right hand side of formula (26) takes the form

$$\frac{\text{trace}\,\eta_D^3(1)}{6} + \frac{\text{trace}\,\eta_D^3(c_2)}{2} + \frac{\text{trace}\,\eta_D^3(c_3)}{3}. \tag{40}$$

Set

$$\beta_1 = b_1 - b_2 + 1 \qquad \beta_2 = b_2 - b_3 + 1. \tag{41}$$

Since $b_1 + b_2 + b_3 = 3p$, we see that

$$\beta_1 - \beta_2 = b_1 - 2b_2 + b_3 = 3(p - b_2) \equiv 0 \pmod 3.$$

Hence $(b_1 + 2, b_2 + 1, b_3) = (\beta_1 + \beta_2 + b_3 - p, \beta_2 + b_3 - p, b_3)$ is a permutation of $(2, 1, 0)$ mod 3 if and only if β_1 or β_2 is not divisible by 3. More precisely, it is an even permutation if $\beta_i \equiv 1 \bmod 3$, and is an odd permutation if $\beta_i \equiv 2 \bmod 3$. Thus we can say

$$\text{trace}\,\eta_D^3(c_3) = \begin{cases} 0 & \text{if } \beta_1 \equiv 0 \pmod 3, \\ 1 & \text{if } \beta_1 \equiv 1 \pmod 3, \\ -1 & \text{if } \beta_1 \equiv -1 \pmod 3. \end{cases} \tag{42}$$

$$= \frac{\omega^{\beta_1} - \omega^{-\beta_1}}{\omega - \omega^2} = \frac{\omega^{\beta_1} - \omega^{-\beta_1}}{\sqrt{3}i} = \frac{2}{\sqrt{3}} \text{Im}\,\omega^{\beta_1}$$

where $\omega = \exp[(2\pi i)/3]$.

The elements 1 and c_2 can be taken to belong to $GL_2 \times GL_1 \subseteq GL_3$. Hence in dealing with them we can use the reduction formula (35). By the standard Branching Rule [25] we have

$$\sigma_D^3 | GL_2 \times GL_1 \simeq \sum \sigma_{(d_1, d_2)}^2 \times \sigma_{d_3}^1, \tag{43a}$$

where (d_1, d_2, d_3) satisfy

$$b_1 \geqslant d_1 \geqslant b_2 \geqslant d_2 \geqslant b_3 \quad d_1 + d_2 + d_3 = 3p. \tag{43b}$$

The only summands of (43a) which are relevant for our own computation are those for which $d_3 = \mathrm{p}$. Thus we have

$$\begin{aligned} \operatorname{trace} \eta_D^3(1) &= \sum_{d_1 + d_2 = 2p} \operatorname{trace} \eta^2_{(d_1, d_2)}(1) \\ &= \sum_{d_1 + d_2 = 2p} 1. \end{aligned} \tag{44}$$

If $b_2 \geqslant p$, then $b_1 \geqslant d_1 \geqslant b_2$ implies $d_2 = 2p - d_1 \leqslant b_2$, $b_3 = 3p - b_1 - b_2 = (2p - b_1) + (p - b_2) \leqslant d_2$. That is, $b_3 \leqslant d_2 \leqslant b_2$ automatically. Hence there are $b_1 - b_2 + 1 = \beta_1$ terms in the sum (44). Similar reasoning in the case $b_2 \leqslant p$ shows that

$$\operatorname{trace} \eta_D^3 = \min(\beta_1, \beta_2). \tag{45}$$

Here β_1 is as defined in (41)

Similarly, using (38) we have

$$\begin{aligned} \operatorname{trace} \eta_D^3(c_2) &= \sum_{d_1 + d_2 = 2p} \operatorname{trace} \eta^2_{(d_1, d_2)}(c_2) = \sum_{d_1 + d_2 = 2p} (-1)^{d_2} \\ &= \sum_{d_1 + d_2 = 2p} (-1)^{d_1}. \end{aligned} \tag{46}$$

From the discussion just above, we know that either d_1 ranges between b_1 and b_2, or d_2 ranges between b_2 and b_3, according as $b_2 \geqslant p$ or $b_2 \leqslant p$. Performing the summation according to cases we find

$$\operatorname{trace} \eta_D^3(c_2) = (-1)^{b_2} \frac{(1 - (-1)^{\min(\beta_1, \beta_2)})}{2}. \tag{47}$$

Plugging (47), (45) and (42) into (40) gives

$$\text{(a)} \qquad \dim \operatorname{Hom}(\sigma_D^n, S^3(\mathbb{C}^n))^{GL_n} = \frac{\beta}{6} + (-1)^{b_2} \frac{(1 - (-1)^{\beta})}{4} + \frac{2\sqrt{3}}{9} \operatorname{Im} \omega^{\beta} \tag{48a}$$

where $D = (b_1, b_2, b_3)$, and

$$\text{(b)} \qquad \beta = \min(\beta_1, \beta_2) \tag{48b}$$

with β_i as in (41). It is routine to check that this formula agrees with statements (4.7), (4.10) of [1].

The case $l = 4$ is considerably more involved than the $l = 2, 3$ situation, and the calculations do get somewhat tedious. Here we will outline what is involved in the computations and list our answers. The details are available from the author on request. The author does hope someone will check the calculations, because he does not have a great deal of faith in his ability to carry through the details in a fault-free manner. He hopes however that the answers are qualitatively correct as stated.

There are 5 conjugacy classes in S_4, specified by elements c_4, c_2c_2, c_3, c_2 and 1. The specialization of the right hand side of formula (26) to the case $l = 4$ is

$$\frac{\operatorname{trace}\eta_D^4(1)}{24} + \frac{\operatorname{trace}\eta_D^4(c_2)}{4} + \frac{\operatorname{trace}\eta_D^4(c_3)}{3} + \frac{\operatorname{trace}\eta_D^4(c_2c_2)}{8} + \frac{\operatorname{trace}\eta_D^4(c_4)}{4}. \quad (49)$$

Here D is a partition of depth 4, and of size $4p$.

$$D = (b_1, b_2, b_3, b_4) \quad b_1 \geqslant b_2 \geqslant b_3 \geqslant b_4 \quad \sum b_i = 4p. \quad (50)$$

The class c_4 is handled by formula (29); we restate this.

$$\operatorname{trace}\eta_D^4(c_4) = \varepsilon(D) = \begin{cases} 1 & \text{according as } (a_1+3, a_2+2, a_3+1, a_4) \pmod 4 \\ -1 & \text{are an even permutation, and odd permutation,} \\ 0 & \text{or not a permutation of } (3,2,1,0) \pmod 4. \end{cases} \quad (51)$$

The class c_2c_2 can be handled by the methods of §3.3 or §3.4, which coincide in this case, but here we will use a different technique which is less systematic but which can be more efficient in some situations because it allows quicker handling of the several subcases which occur.

We appeal directly to the Character Formula (28), but instead of computing simply trace $\sigma_D^4(c_2c_2)$, we compute trace $\sigma_D^4(c_2c_2a)$ where a is a general element of A_4. This will be a polynomial in the coefficients a_1, a_2, a_3, a_4 of a, and the coefficient of $(a_1a_2a_3a_4)^p$ will be trace $\eta_D^4(c_2c_2)$.

Consider an element

(a)
$$c_2c_2a = \begin{bmatrix} 0 & a_2 & 0 & 0 \\ a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a_4 \\ 0 & 0 & a_3 & 0 \end{bmatrix}. \quad (52a)$$

This will have eigenvalues $\pm(a_1a_2)^{1/2}$, $\pm(a_3a_4)^{1/2}$. Set

(b)
$$\gamma = (a_1a_2)^{1/2} \quad \delta = (a_3a_4)^{1/2}. \quad (52b)$$

Then the numerator of (28) for $x = c_2c_2a$ and D from (50) is

$$\begin{bmatrix} \gamma^{b_1+3} & \gamma^{b_2+2} & \gamma^{b_3+1} & \gamma^{b_4} \\ (-\gamma)^{b_1+3} & (-\gamma)^{b_2+2} & (-\gamma)^{b_3+1} & (-\gamma)^{b_4} \\ \delta^{b_1+3} & \delta^{b_2+2} & \delta^{b_3+1} & \delta^{b_4} \\ (-\delta)^{b_1+3} & (-\delta)^{b_2+2} & (-\delta)^{b_3+1} & (-\delta)^{b_4} \end{bmatrix}. \quad (53)$$

By inspection, we see that if any 3 of the exponents b_1+3, b_2+2, b_3+1, b_4 have the same parity, then (53) vanishes identically. Hence two exponents must be even and two must be odd. Let r_1, r_2 be the even exponents, with $r_1 > r_2$, and let q_1, q_2 be the

even exponents with $q_1 > q_2$. We calculate

$$\det\begin{bmatrix} \gamma^{r_1} & \gamma^{r_2} & \gamma^{q_1} & \gamma^{q_2} \\ \gamma^{r_1} & \gamma^{r_2} & -\gamma^{q_1} & -\gamma^{q_2} \\ \delta^{r_1} & \delta^{r_2} & \delta^{q_1} & \delta^{q_2} \\ \delta^{r_1} & \delta^{r_2} & -\delta^{q_1} & -\delta^{q_2} \end{bmatrix} = 4\det\begin{bmatrix} 0 & 0 & \gamma^{q_1} & \gamma^{q_2} \\ \gamma^{r_1} & \gamma^{r_2} & 0 & 0 \\ 0 & 0 & \delta^{q_1} & \delta^{q_2} \\ \delta^{r_1} & \delta^{r_2} & 0 & 0 \end{bmatrix}$$

$$= -4\det\begin{bmatrix} \gamma^{r_1} & \gamma^{r_2} & 0 & 0 \\ \delta^{r_1} & \delta^{r_2} & 0 & 0 \\ 0 & 0 & \gamma^{q_1} & \gamma^{q_2} \\ 0 & 0 & \delta^{q_1} & \delta^{q_2} \end{bmatrix}$$

$$= -4(\gamma\delta)^{r_2+q_2}(\gamma^{r_1-r_2} - \delta^{r_1-r_2})(\gamma^{q_1-q_2} - \delta^{q_1-q_2}).$$

The denominator of (28) for $x = c_2c_2a$ can be calculated to be $4\gamma\delta(\gamma^2 - \delta^2)^2$. Thus the value of (28) is

(a) $$\operatorname{trace}\sigma_D^4(c_2c_2a) = \pm(\gamma\delta)^{r_2+q_2-1}\left(\sum_{j=0}^{r}\gamma^{2(r-j)}\delta^{2j}\right)\left(\sum_{k=0}^{q}\gamma^{2(q-k)}\delta^{2k}\right) \tag{54a}$$

where

(b) $$r = (r_1 - r_2 - 2)/2, \quad q = (q_1 - q_2 - 2)/2 \tag{54b}$$

(c) The $\pm$ sign is $-\operatorname{sgn}(s)$ where s is the permutation that takes

$$(b_1 + 3,\ b_2 + 2,\ b_3 + 1,\ b_4) \text{ to } (r_1, r_2, q_1, q_2). \tag{54c}$$

To compute trace $\eta_D^4(c_2c_2)$ we look for the coefficient of $(\gamma\delta)^{((r_1+r_2+q_1+q_2)/2)-3}$. This is $\pm$ the coefficient of $(\gamma\delta)^{r+q}$ in the product

$$\left(\sum_{j=0}^{r}\gamma^{2(r-j)}\delta^{2j}\right)\left(\sum_{k=0}^{q}\gamma^{2(q-k)}\delta^{2k}\right).$$

Note that $r + q = 2p - (r_2 + q_2 - 1)$ is even, so that $(\gamma\delta)^{r+q}$ does occur in the expansion of this product. And indeed, we can see fairly easily that it appears with the coefficient $\min(r+1, q+1)$. Thus we arrive at the following description of trace $\eta_D^4(c_2c_2)$.

(a) trace $\eta_D^4(c_2c_2) = 0$ unless two of the numbers
$(b_1 + 3,\ b_2 + 2,\ b_3 + 1,\ b_4)$ are even, and two are odd. (55a)

(b) If the non-vanishing criterion of (a) is satisfied, let
r_1, r_2 denote the even pair, with $r_1 > r_2$, and let
$q_1 > q_2$. Let s be the permutation (55b)

$$(b_1 + 3, b_2 + 2, b_3 + 1, b_4) \xrightarrow{s} (q_1, r_1, q_2, r_2).$$

Then

$$\operatorname{trace}\eta_D^4(c_2c_2) = \operatorname{sgn}(s)(\min(r_1 - r_2, q_1 - q_2))/2. \tag{55c}$$

The classes c_3, c_2, and 1 all may be considered to be elements of $GL_3 \times GL_1 \subseteq GL_4$, so they may be treated via the method of § 3.4, using the formulas for $l = 3$ and the Branching Rule

$$\text{(a)} \qquad \sigma_D^4 | GL_3 \times GL_1 = \sum_{d_i} \sigma^3_{(d_1,d_2,d_3)} \otimes \sigma^1_{d_4}, \tag{56a}$$

where the d_i satisfy

$$\text{(b)} \qquad b_1 \geqslant d_1 \geqslant b_2 \geqslant d_2 \geqslant b_3 \geqslant d_3 \geqslant b_4 \quad \sum d_i = \sum b_i = 4p. \tag{56b}$$

Hence the b_i define D—see definition (50). We have seen that only the summands such that

$$\text{(c)} \qquad d_1 + d_2 + d_3 = 3p \quad d_4 = p \tag{56c}$$

contribute to trace η_D^4. Thus to compute trace $\eta_D^4(x)$ for $x = 1$, c_2 and c_3, we just plug quantities (45), (47), or (42) into (35), and sum over the appropriate (d_1, d_2, d_3).

In evaluating the sum, we must distinguish several cases.

$$\text{(a)} \qquad \text{Case I:} \quad b_3 \geqslant p. \quad \text{This implies} \quad d_2 \geqslant p, \quad \text{so that} \tag{57a}$$

$$\beta = \min(d_1 - d_2, d_2 - d_3) + 1 = d_1 - d_2 + 1$$

Further, if $b_1 \geqslant d_1 \geqslant b_2 \geqslant d_2 \geqslant b_3$, then $b_4 = 4p - b_1 - b_2 - b_3 \leqslant 3p - d_1 - d_2 = d_3 \leqslant 3p - b_2 - b_3 \leqslant p \leqslant b_3$. Hence d_3 is automatically in the correct range.

$$\text{(b)} \qquad \text{Case II:} \quad b_2 \leqslant p. \text{ With reasoning similar to Case 1, we find} \tag{57b}$$

$$\beta = d_2 - d_3 + 1$$

and if $b_2 \geqslant d_2 \geqslant b_3 \geqslant d_3 \geqslant b_4$, then $b_1 \geqslant d_1 \geqslant b_2$ automatically.

$$\text{(c)} \qquad \text{Case III:} \quad b_3 \leqslant p \leqslant b_2. \quad \text{In this case we can have}$$

$$\beta = d_1 - d_2 + 1 \quad \text{if} \quad d_2 \geqslant p \quad \text{iff} \quad d_1 + d_3 \leqslant 2p \tag{57c}$$

or

$$\beta = d_2 - d_3 + 1 \quad \text{if} \quad d_2 \leqslant p \quad \text{iff} \quad d_1 + d_3 \geqslant 2p.$$

In this case we use d_1 and d_3 to parametrize the relevant Young Diagrams (d_1, d_2, d_3) satisfying (56b, c). The pair (d_1, d_3) must satisfy

$$b_2 \leqslant d_1 \leqslant b_1 \quad b_4 \leqslant d_3 \leqslant b_3$$

$$3p - b_2 \leqslant d_1 + d_3 \leqslant 3p - b_3.$$

It appears initially in Case III that there are 12 subcases that need to be considered. However, some happy cancellations reduce the final results to two only situations, according as $b_1 - b_2 \leqslant b_3 - b_4$ or $b_1 - b_2 \geqslant b_3 - b_4$.

To compute trace $\eta_D^4(1)$ we must sum, over the ranges indicated above:

$$\text{(a)} \qquad \text{In Case I:} \quad \sum_{d_1, d_2} d_1 - d_2 + 1. \tag{58a}$$

(b) In Case II: $$\sum_{d_2,d_3} d_2 - d_3 + 1, \tag{58b}$$

(c) In Case III: $$\sum_{d_1+d_3\le 2p} (2d_1 + d_3 - 3p + 1) + \sum_{d_1+d_3>2p} (3p - d_1 - 2d_3 + 1). \tag{58c}$$

To compute trace $\eta_D^4(c_2)$ we must sum, over the ranges indicated above:

(a) In Case I: $$\sum_{d_1,d_2} ((-1)^{d_1} + (-1)^{d_2})/2. \tag{59a}$$

(b) In Case II: $$\sum_{d_2,d_3} ((-1)^{d_2} + (-1)^{d_3})/2. \tag{59b}$$

(c) In Case III: $$\sum_{d_1+d_3\le 2p} ((-1)^{d_1} + (-1)^{p+d_1+d_3})/2 \tag{59c}$$
$$+ \sum_{d_1+d_3>2p} ((-1)^{d_3} + (-1)^{p+d_1+d_3})/2.$$

To compute trace $\eta_D^4(c_2)$, we must sum, over the ranges indicated above:

(a) In Case I: $$\sum_{d_1,d_2} \frac{2}{3}\sqrt{3}\,\mathrm{Im}\,\omega^{d_1-d_2+1}. \tag{60a}$$

(b) In Case II: $$\sum_{d_2,d_3} \frac{2}{3}\sqrt{3}\,\mathrm{Im}\,\omega^{d_2-d_3+1}. \tag{60b}$$

(c) In Case III: $$\sum_{d_1,d_3} \frac{2}{3}\sqrt{3}\,\mathrm{Im}\,\omega^{-(d_1-d_3+1)}. \tag{60c}$$

We record the results of these calculations.

Notation: Set $\beta_1 = b_1 - b_2 + 1$, $\beta_2 = b_2 - b_3 + 1$ and $\beta_3 = b_3 - b_4 + 1$ (61

Then trace $\eta_D^4(1)$ (= dimension of the zero-weight space) is equal to:

(a) In Case I: $$\beta_1\beta_2(\beta_1+\beta_2)/2, \tag{62a}$$

(b) In Case II: $$\beta_2\beta_3(\beta_2+\beta_3)/2, \tag{62b}$$

(c) In Case III: $$\frac{\beta_1\beta_2\beta_3}{2} + \frac{\beta_3}{8}(2-(\beta_1-\beta_3))(2+\beta_1-\beta_3) \quad \text{if} \quad \beta_1 > \beta_3$$
$$\frac{\beta_1\beta_2\beta_3}{2} + \frac{\beta_1}{8}(2-(\beta_1-\beta_3))(2+\beta_1-\beta_3) \quad \text{if} \quad \beta_1 < \beta_3. \tag{62c}$$

For the next set of formulas we use the notation

(a) $$\sigma(x) = \sin^2(\pi x/2). \tag{63a}$$

Note $\sigma(2k) = 0$ if k is an integer, and $\sigma(2k+1) = 1$. For integers n, we can also writ

(b) $$\sigma(n) = \frac{1-(-1)^n}{2}, \quad n \in \mathbb{Z}. \tag{63b}$$

trace $\eta_D^4(c_2)$ is equal to:

(a) In Case I: $$\frac{(-1)^{b_2}}{2}(\sigma(\beta_1)\beta_2 + \sigma(\beta_2)\beta_1). \tag{64a}$$

(b) In Case II: $$\frac{(-1)^{b_2}}{2}(\sigma(\beta_3)\beta_2 + \sigma(\beta_2)\beta_3). \tag{64b}$$

(c) In Case III:

$$\frac{(-1)^{p+b_1+b_3}}{2}\sigma(\beta_1)\sigma(\beta_3) + (-1)^{b_4}\frac{(\sigma(\beta_3)(\beta_1+\beta_3) - 2\sigma(\beta_2+\beta_3)\beta_3)}{4} \quad \text{if} \quad \beta_1 \geqslant \beta_3$$

$$\frac{(-1)^{p+b_1+b_3}}{2}\sigma(\beta_1)\sigma(\beta_3) + (-1)^{b_1}\frac{(\sigma(\beta_1)(\beta_1+\beta_3) - 2\sigma(\beta_1+\beta_2)\beta_1)}{4} \quad \text{if} \quad \beta_1 \leqslant \beta_3. \tag{64c}$$

Finally we have trace $\eta_D^4(c_3)$ is equal to:

(a) In Case I: $$\frac{-2\sqrt{3}}{9}\operatorname{Im}(1-\omega^{\beta_1})(1-\omega^{\beta_2}) = \begin{cases} 1 & \text{if} \quad \beta_1, \beta_2 = 1 \pmod 3 \\ -1 & \text{if} \quad \beta_1, \beta_2 \equiv 2 \pmod 3 \\ 0 & \text{otherwise.} \end{cases} \tag{65a}$$

(b) In case II: $$\frac{-2\sqrt{3}}{9}\operatorname{Im}(1-\omega^{\beta_2})(1-\omega^{\beta_3}) = \begin{cases} 1 & \text{if} \quad \beta_2, \beta_3 \equiv 1 \pmod 3 \\ -1 & \text{if} \quad \beta_2, \beta_3 \equiv 2 \pmod 3 \\ 0 & \text{otherwise.} \end{cases} \tag{65b}$$

(c) In Case III: $$\frac{-2\sqrt{3}}{9}\operatorname{Im}(\omega^{-\beta_2}(1-\omega^{\beta_1})(1-\omega^{-\beta_3})). \tag{65c}$$

3.6: *Remarks*:

(a) The method of § 3.1 for computing $S^l \circ S^p$ may seem unduly cumbersome: it requires one to compute a number for every partition of l. If one is interested in a particular l, p and D, there may well be a simpler route to the answer. However, the radically different behaviour of the various terms in the sum (26), as seen in the examples of $l = 2, 3, 4$, leads one to surmise that (26) is a fairly efficient decomposition of the multiplicity function $\dim \operatorname{Hom}(\sigma_D^n, S^l(S^p(\mathbb{C}^n)))$ into reasonably computable pieces. This of course is what Fourier Analysis aspires to.

(b) If one does the hard work to compute $S^l \circ S^p$ by formula (26), then as a dividend, one gets, more or less at no extra cost, all other plethysms $S^D \circ S^p$, with $|D| = l$, simply by averaging the terms trace $\eta_D^4(x)$ over the other characters of S_l.

(c) The reasonably clean form of the individual terms in the expansion (49), especially the neatness of the cancellations which lead to compact answers in Case III for trace $\eta_D^4(x)$, $x = 1, c_2, c_3$, give one hope that these calculations could be carried further, to $l = 5$ at least, and perhaps beyond.

(d) One expects from the discussion of §3.2–3.4 that when D is large in a suitable sense, the main contribution to the sum in (26) will come from the identity element. In other words, asymptotically as p, $D \to \infty$ in a suitable sense, the multiplicity of σ_D^n in $S^l(S^p(\mathbb{C}^n))$ is approximately

$$\dim V_D^0/l!,$$

where V_D^0 denotes the dimension of the zero weight space in σ_D^l. This number, in turn, has an asymptotic approximation in terms of symplectic geometry [6]. It might be interesting to make these asymptotic relations explicit.

The dominance of the term trace $\eta_D^4(1)/l!$ is clear in our examples. In formula (48), the contributions the terms for c_2 and c_3 is less than 1—in fact, at most 7/12. Of the terms in (49), the identity term is a cubic polynomial in the entries of D, the terms for c_2 and c_2c_2 are linear polynomials, and the terms for c_3 and c_4 are bounded independent of D.

(e) In connection with remark (d), we can observe that there are D for which only the identity term of (26) gives a non-zero contribution. Indeed, let $D = (b_1, b_2, \ldots, b_l)$, and suppose that the numbers $b_i + l - i$ are all congruent modulo $l!$ If l is odd, it is possible to require the b_i to satisfy this and still have $\sum b_i \equiv 0 \bmod l$. Choose $x \in S_l$, and suppose x contains an r-cycle for some $r > 1$. Then any element of the form xa, $a \in A_l$, will have a collection of r eigenvalues of the form $\exp[(2\pi i)j/r]\lambda$, for $0 \leqslant j < r$, and some $\lambda \in \mathbb{C}$. From this and the character formula (28), we can see trace $\sigma_D^l(xa) = 0$. (The rows corresponding to these r eigenvalues in the matrix in the denominator of (28) will all be multiples of each other.) Hence for such D, only the identity element of S_l can contribute to formula (26).

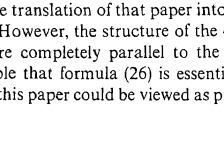
(f) The paper [1] discusses algorithms for plethysm. It is couched in rather different terms from this paper. Its language is heavily combinatorial (D-compatible tableaux, circle diagram, p-slinky, etc.). The translation of that paper into representation theory does not seem straightforward. However, the structure of the explicit calculations in [1], §4, for the cases $l = 2, 3$ are completely parallel to the computations in §3.5 for $l = 2, 3$. Thus it seems possible that formula (26) is essentially equivalent to the algorithm used in [1]. If so, then this paper could be viewed as providing a geometrical interpretation of that algorithm.

4. Invariants

As was mentioned in §2.5, the computation of $S^l(S^p(\mathbb{C}^n)$ amounts in classical terms to the description of covariants of an n-ary p-ic. In this connection, special interest attaches to the (relative) invariants, i.e. the occurrence of $(\det_n)^k$ in $S^l(S^p(\mathbb{C}^n))$. In this section we will make a few observations bearing on the invariants.

4.1: Let $\Delta_{l,k}$ denote the Young Diagram consisting of l rows of length k.

(a)

$\Delta_{l,k} = l$ 

(66a)

Consider the representations

$$\text{(b)} \qquad \sigma^n_{\Delta_{l,k}} = \sigma^n_{l\times k}. \tag{66b}$$

The representation $\sigma^n_{l\times 1}$ is the l-th fundamental representation of GL_n, realized by the natural action on $\Lambda^l(\mathbb{C}^n)$, the l-th exterior power of $\mathbb{C}^n$. In particular

$$\sigma^n_{n\times 1} = \det_n \tag{67}$$

is the determinant character of GL_n. The representation $\sigma^n_{l\times k}$ is the k-th Cartan power of $\sigma^n_{l\times 1}$. In particular $\sigma^n_{n\times k} = (\det_n)^k$.

The only irreducible representations of GL_n which contain fixed vectors for SL_n are the powers of $\det_n$. Thus we can see from the decomposition (2) that the space of SL_n-fixed vectors in $S(\mathbb{C}^n\otimes\mathbb{C}^l)$ has a decomposition

$$\mathbb{S}(\mathbb{C}^n\otimes\mathbb{C}^l)^{SL_n} \simeq \sum_{k\geqq 0} (\det_n)^k \otimes \sigma^l_{n\times k} \tag{68}$$

as $(GL_n \times GL_l)$-module. Since $\det_n$ is a one-dimensional representation, the homogeneous summands of the sum (68) are irreducible as GL_l-modules. It follows that the algebra $\mathbb{S}(\mathbb{C}^n\otimes\mathbb{C}^l)^{SL_n}$ is generated by its lowest-positive-degree subspace, $\det_n \otimes \sigma^l_{n\times 1}$. By the Weyl Dimension Formula

$$\text{(a)} \qquad \dim \sigma^l_{n\times k} = \prod_{a=1}^{n} \frac{(l+k-a)!\,(n-a)!}{(n+k-a)!\,(l-a)!} = \prod_{a=1}^{n} \frac{\binom{l+k-a}{l-n}}{\binom{l-a}{l-n}}$$

$$= \prod_{a=1}^{n} \frac{\binom{l+k-a}{k}}{\binom{n+k-a}{k}}. \tag{69a}$$

As $k\to\infty$, this is asymptotic to

$$\text{(b)} \qquad (n(l-n))!\left(\prod_{a=1}^{n}\frac{(n-a)!}{(l-a)!}\right)\frac{k^{n(l-n)}}{(n(l-n))!}. \tag{69b}$$

This is the coordinate ring of the Grassmann variety of n-planes in l-space, a projective variety of dimension $n(l-n)$. These observations throw some geometric light on the remarks following Theorem 7.6, page 207 in [24].

4.2: Let $\det_l$ denote also the restriction of the determinant character of GL_l to the maximal torus A_l, and let χ_l be the extension of $\det_l$ to $S_l \circledS A_l$ discussed in §2.5 (see formula (20)). We have seen in §2.5 that

$$S^l(S^p(\mathbb{C}^n)) \simeq S(\mathbb{C}^n\otimes\mathbb{C}^l)^{(\chi_l)^p}, \tag{70}$$

where $S(\mathbb{C}^n\otimes\mathbb{C}^l)^{(\chi_l)^p}$ denotes the $(\chi_l)^p$-isotypic component for the action of $S_l \circledS A_l$ on $S(\mathbb{C}^n\otimes\mathbb{C}^l)$. Further, the isomorphism (70) is an isomorphism of GL_n-modules. It

follows that

$$\sum_{p\geq 0} S^l(S^p(\mathbb{C}^n)^{SL_n} \simeq \sum_{k=0} \det_n^k \otimes (\sigma^l_{n\times k})^{(\chi_l)^p}, \tag{71}$$

where $pl = nk$. In particular we have an algebra structure on $\sum_{p\geq 0} S^l(S^p(\mathbb{C}^n))^{SL_n}$.

The $(\chi_l)^p$-isotypic component $(\sigma^l_{n\times k})^{(\chi_l)^p}$ of $\sigma^l_{n\times k}$ is of course contained in the zero weight space

$$(\sigma^l_{n\times k})^{A_l,(\det_l)^p} = (\sigma^l_{n\times k})^{A_l^1}$$

of fixed vectors for $A_l^1 = A_l \cap SL_n$ (see § 3.1). The sum of the zero weight spaces is again an algebra, the algebra of joint invariants for SL_n and for A_l^1. Using Corollary (13), we have

$$S(\mathbb{C}^n \otimes \mathbb{C}^l)^{SL_n \times A_l^1} \simeq \sum_{k\geq 0} (\det_n)^k \otimes (\sigma^l_{n\times k})^{A_l^1} \simeq \sum_{pl=nk} T^l(S^p(\mathbb{C}^n))^{SL_n} \tag{72}$$

This algebra allows an action of S_l, and the algebra (71) is the subalgebra of S_l invariants in (72).

In the case $n = 2$, the algebra (72) is much easier to describe than (71). In particular, one can show that when $n = 2$ algebra (72) is generated by its elements of at least positive degree ([15]; see also [17], [7]). It would be interesting to know if this holds for larger n.

When $n = 2$, one can also give an explicit formula for the dimension of $(\sigma^l_{n\times k})^{A_l^1}$. For general n one has Kostant's formula [12], but this does not immediately give one the control one might like to have on these dimensions. For example, since the algebra (72) defines a projective variety of dimension $n(l-n)-(l-1)$ we know that asymptotically as $p\to$, subject to $pl = nk$,

$$\dim T^l(S^p(\mathbb{C}^n))^{SL_n} \simeq \gamma \frac{p^{n(l-n)-l+1}}{(n(l-n)-l+1)!} \tag{73}$$

for an appropriate constant γ. It would be nice to evaluate γ. One would then know, by the asymptotic philosophy of Remark (d) in § 3.6, or more precisely by [11], that

$$\dim (S^l(S^p(\mathbb{C}^n))^{SL_n}) \simeq \frac{\gamma}{l!} \frac{p^{n(l-n)-l+1}}{(n(l-n)-l+1)!} \tag{74}$$

since $|S_l| = l!$. This method is used in [7] to derive Hilbert's asymptotic estimate for the number of invariants of degree p for a binary form.

4.3: Using (71) and some elementary duality considerations we can draw some conclusions about invariants of low degree

PROPOSITION:

(a) $$S^l(S^p(\mathbb{C}^n))^{SL_n} = \{0\} \quad \text{if} \quad l < n. \tag{75a}$$

(b) $$S^n(S^p(\mathbb{C}^n))^{SL_n} = \begin{cases} 0 & \text{if } p \text{ is odd} \\ \mathbb{C} & \text{if } p \text{ is even} \end{cases} \tag{75b}$$

Proof. Statement (a) is obvious since the Young Diagram $\Delta_{n,k}$ corresponding to $(\det_n)^k$ cannot occur in decomposition (2) if $l < n$. For statement (b), we note if $l = n$, then $\sigma^l_{n\times k} \simeq (\det_l)^k$. The character χ_l of $S_l \circledS A_l$ has the form

$$\chi_l \simeq \operatorname{sgn} \otimes \det_l, \tag{76}$$

where $\det_l$ denotes the restriction to $S_l \circledS A_l$ of the determinant character of GL_l, and sgn is the signum character of S_l, extended to $S_l \circledS A_l$ by the quotient map

$$1 \to A_l \to S_l \times A_l \to S_l \to 1.$$

Hence $(\det_l)^k$ restricted to $S_l \times A_l$ agrees with $(\chi_l)^k$ precisely when k is even. Conclusion (b) follows.

We can draw some conclusions for $l > n$ by the following simple contragredience relations for the representations $\sigma^l_{n\times k}$. We have

$$(\sigma^l_{n\times k})^* \simeq \sigma^l_{(l-n)\times k} \otimes (\det_l)^{-k}, \tag{77}$$

where $*$ denotes contragredient. Since $S_l \circledS A_l$ is acting reductively we have,

(a)
$$((\sigma^l_{n\times k})^{(\chi_l)^p})^* \simeq ((\sigma^l_{n\times k})^*)^{(\chi_l)^{-p}} \simeq (\sigma^l_{(l-n)\times k} \otimes (\det_l)^{-k})^{(\chi_l)^{-p}}$$
$$\simeq (\sigma^l_{(l-n)\times k})^{(\chi_l)^{-p}(\det_l)^k}. \tag{78a}$$

For the first space in (78a) to be non-zero, we need

(b)
$$pl = kn \tag{78b}$$

Assuming this holds, we see that if k is *even*

$$(\chi_l)^{-p}(\det_l)^k = \chi_l^q,$$

where

(c)
$$-p + k = q, \quad \text{whence} \quad ql = (l-n)k. \tag{78c}$$

We conclude from (71) and (77):

PROPOSITION:

If k is even, $p + q = k$, and $pl = nk$, $ql = (l-n)k$, or $qn = p(l-n)$, there is a natural duality between the spaces

$$S^l(S^p(\mathbb{C}^n))^{SL_n} \quad \text{and} \quad S^l(S^q(\mathbb{C}^{l-n}))^{SL_{l-n}}. \tag{79}$$

In particular, these spaces have the same dimension.

Take $l = n+1$. The zero weight space of $\sigma^{n+1}_{1\times k} \simeq S^k(\mathbb{C}^{n+1})$ is non-trivial if and only if $k = a(n+1)$ for some integer a; when it is non-zero, it has dimension 1, and defines an invariant for S_{n+1}. Applying the above proposition and (78a) we conclude

$$\dim S^{n+1}(S^p(\mathbb{C}^n))^{SL_n} = \begin{cases} 0 & \text{unless} \quad p = nq \text{ with } (n+1)q \text{ even} \\ 1 & \text{if} \quad p = nq, \quad \text{with } (n+1)q \text{ even.} \end{cases} \tag{80}$$

Take $l = n + 2$. We can conclude

$$\dim S^{n+2}(S^p(\mathbb{C}^n))^{SL_n}$$

$$= \begin{cases} 0 & \text{unless} \quad p(n+2) = nk \quad \text{for some} \quad k \in \mathbb{Z} \\ \dim S^{n+2}(S^{2k/(n+2)}(\mathbb{C}^2)) & \text{if} \quad k \in 2\mathbb{Z} \cap \left(\dfrac{n+2}{2}\right)\mathbb{Z}. \end{cases} \tag{81}$$

4.4: Finally, we observe that [7], Theorem 5.8 generalizes from binary invariants to n-ary invariants. Consider the graded algebra

$$\text{(a)} \qquad \mathscr{I}_{n,p} = S(S^p(\mathbb{C}^n))^{SL_n} \simeq \sum_{l \geqslant 0} S^l(S^p(\mathbb{C}^n))^{SL_n} = \sum_{l \geqslant 0} I^l_{n,p} \tag{82a}$$

of invariants of the n-ary p-ic. Let

$$\text{(b)} \qquad \mathscr{I}^+_{n,p} = \sum_{l \geqslant 1} I^l_{n,p} \tag{82b}$$

be the ideal of elements of $\mathscr{I}_{n,p}$ without constant term. Then the graded quotient

$$\text{(c)} \qquad \mathscr{I}^+_{n,p}/(\mathscr{I}^+_{n,p})^2 \simeq \sum_{l \geqslant 1} I^l_{n,p}/((\mathscr{I}^+_{n,p})^2 \cap I^l_{n,p}) \tag{82c}$$

is called the *space of fundamental generators* for $\mathscr{I}_{n,p}$. One observes that any set $Y = \{y_i\}$ of generators for $\mathscr{I}_{n,p}$ as algebra must satisfy $|Y| \geqslant \dim(\mathscr{I}^+_{n,p}/(\mathscr{I}^+_{n,p})^2)$. Since

$$(\mathscr{I}^+_{n,p})^2 \cap I^l_{n,p} = \sum_{\substack{a+b=l \\ a,b<l}} I^a_{n,p} I^b_{n,p}$$

we see that

$$\dim(I^l_{n,p})/((\mathscr{I}^+_{n,p})^2 \cap I^l_{n,p}) \geqslant \dim I^l_{n,p} - \sum_{\substack{a+b=l \\ a,b<l}} \dim I^a_{n,p} \dim I^b_{n,p}.$$

From the asymptotic formula (74) for $S^l(S^p(\mathbb{C}^n))$, we see that as $p \to \infty$, the value of the sum over a, b is negligible in comparison with $\dim I^l_{n,p}$. Thus we arrive at the following conclusion.

Theorem. *For fixed n and $l \geqslant n$, as $p \to \infty$ subject to $pl = nk$ for some $k \in \mathbb{Z}$, the ratio of the dimension of the fundamental invariants in $I^l_{n,p}$ to $\dim I^l_{n,p}$ approaches* 1.

Thus loosely speaking, as $p \to \infty$, almost all low degree invariants of the n-ary p-ic are fundamental invariants.

References

[1] Chen Y, Garsia A and Remmel J, Algorithms for plethysm in combinatorics and algebra, *Contemp. Math. AMS Providence RI* **34** (1984) 109–153

[2] Curtis C and Reiner I, *Representation theory of finite groups and associative algebras* (New York: Wiley-Interscience) (1962)

[3] Duncan D, On D E Littlewood's algebra of S-functions, *Can. J. Math.* **4** (1952) 504–512

[4] Foulkes H, Concomitants of the quintic and sextic up to degree four in coefficients of the ground form. *J. London Math. Soc.* **25** (1950) 205–209
[5] Gross K and Kunze R, Bessel functions and representation theory II. Holomorphic discrete series and metaplectic representations, *J. Funct. Anal.* **25** (1977) 1–49
[6] Guillemin V. and Sternberg S, The Frobenius reciprocity theorems from a symplectic point of view in *Nonlinear partial differential operators and quantization procedures, Lecture notes in math.* No. 1037 (New York: Springer-Verlag) 1983, pp. 212–256
[7] Howe R, The classical groups and invariants of binary forms in: *Proceedings of the Hermann Weyl Centennial Symposium* (Durham: AMS Publication) (1987) (to appear)
[8] Howe R, Remarks on classical invariant theory (preprint)
[9] Howe R, Transcending classical invariant theory (preprint)
[10] Howe R, Reciprocity laws in the theory of dual pairs, in: *Representation theory of reductive groups, Progress in mathematics* (ed.) P Trombi (Boston: Birkhauser) vol 40 (1983) pp. 159–175
[11] Howe R, Asymptotic dimensions of spaces of invariants (in preparation)
[12] Jacobson N, *Lie algebras* (New York: Interscience Publishers) 1962
[13] James G D, The representation theory of the symmetric groups, *Lecture notes in mathematics*, No. 682 (New York: Springer-Verlag) (1978)
[14] Kashiwara M and Vergne M, On the Segal–Shale–Weil representations and harmonic polynomials, *Invent. Math.* **44** (1978) 1–47
[15] Kempe A, On regular difference terms, *Proc. London Math. Soc.* **25** (1894) 465–470
[16] Klink W and Ton-That T, Calculation of Clebsch–Gordan and Racah coefficients using symbolic manipulation programs (preprint)
[17] Kung J and Rota G-C, The invariant theory of binary forms, *BAMS (new series)* **10** (1984) 27–85
[18] Lang S, *Algebra* (Reading: Addison–Wesley) (1984)
[19] Littelman P, A decomposition formula for Levi sub-groups (preprint)
[20] Littlewood D, *The theory of group characters and matrix representations of groups* (Oxford: University Press) (1940)
[21] MacDonald I, *Symmetric functions and Hall polynomials* (Oxford: University Press) (1979)
[22] Stanley R, $GL_n(\mathbb{C})$ for combinatorialists, in: *Surveys in combinatorics* (ed.) E K Lloyd (Cambridge: University Press) London Math. Soc. Lecture Notes No. 82 (1983)
[23] Thrall R, On symmetrized Kronecker powers and the structure of the free Lie ring, *Am. J. Math.* **64** (1942) 371–388
[24] Weyl H, *The classical groups* (Princeton: University Press) (1946)
[25] Zhelobenko D, Compact Lie groups and their representations, Trans. Math. Mono. No. 40, AMS Providence (1973)

Note added in proof: I thank I G Macdonald for drawing my attention to the paper
Foulkes H, Plethysms of *S*-functions, *Trans. R. Soc. London* **A246** (1954) 555–593

This paper contains the calculation of §3.5. Although Foulkes's conceptual framework differs from ours, the details of his calculations are quite similar.

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 111–116.
© Printed in India.

The area within a curve

M N HUXLEY
Department of Pure Mathematics, University College, Cardiff, PO Box 78, Cardiff CF1 1XL, UK

Abstract. The area of a simple closed convex curve can be estimated in terms of the number of points of a square lattice that lie within the curve. We obtain the usual error bound without integration using a form of the Hardy–Littlewood–Ramanujan circle method, and also present simple estimates for the mean square error.

Keywords. Estimation of area; lattice points.

1. Introduction

This note treats an old and familiar problem: to estimate the area A within a simple closed convex curve C, drawn on graph paper which carries a square lattice of sides $1/R$. To clear fractions we take the side of the lattice squares as the new unit of length; C has area AR^2 in these units. There are three usual methods of estimating the area. The trapezium rule adds up the distances intercepted by the curve along lattice lines parallel to the y-axis. The lattice squares rule counts the number of lattice squares whose centres lie within the curve. The lattice points rule counts the number of lattice points (crossings of the lattice lines) within the curve. To be more precise, if the curve is given by two equations $y = F(x)$, $y = f(x)$ for $a \leqslant x \leqslant b$, where $f(a) = F(a)$, $f(b) = F(b)$, the trapezium rule estimate is

$$T = \sum_{a \leqslant n \leqslant b} (F(n) - f(n)),$$

and the lattice squares and lattice points estimates are special cases of the integer part sum (in which square brackets denote the integer part)

$$N(u, v) = \sum_{a-u \leqslant n \leqslant b-u} ([F(n+u) - v] - [f(n+u) - v])$$

with $(u, v) = (\frac{1}{2}, \frac{1}{2})$ and $(0, 0)$ respectively.

We write $D(u, v)$ for the discrepancy

$$D(u, v) = N(u, v) - AR^2,$$

and similarly

$$E(u) = T(u) - AR^2 = \sum_{a-u \leqslant n \leqslant b-u} (F(n+u) - f(n+u)).$$

If the curve C is contained in a rectangle with sides parallel to the coordinate axes,

lengths B and H respectively, then it is easy to see geometrically that

$$|E(u)| \leqslant 2H,$$

$$|D(u,v)| \leqslant 2B + 2H + 4.$$

The error bounds on the right are both order of magnitude $O(R)$ as R tends to infinity. If the curve C is itself a rectangle, these bounds cannot be improved. We use the following order of magnitude notation: $g(R) \ll G(R)$ as R tends to infinity means that

$$\limsup_{R\to\infty} \frac{|g(R)|}{G(R)} < \infty.$$

Any term $g(R)$ in an estimate may be replaced by $O(G(R))$, read as 'an error term of order of magnitude $G(R)$'.

From now on we suppose that C is a smooth curve with continuous non-zero radius of curvature. Estimates of the form

$$D(u,v) \ll R^{(2/3)+\alpha} \tag{1}$$

(for any $\varepsilon > 0$) were given by Voronoi, Sierpiński, van der Corput, Landau, Jarnik and Vinogradov, sometimes as special cases only. Jarnik also showed that the exponent 2/3 cannot be reduced without further smoothness conditions. The problem is treated at length in Landau [7] and briefly in Vinogradov [10]. A remark apparently missing from Landau is that the bounds

$$E(u) \ll R^{1/2}, \tag{2}$$

$$\int_0^1 |E(u)|^2 \,\mathrm{d}u \leqslant \int_0^1 \int_0^1 |D(u,v)|^2 \,\mathrm{d}u\,\mathrm{d}v \ll R \tag{3}$$

and, if the curve C is three times differentiable,

$$\int_0^1 |E(u)|^2 \,\mathrm{d}u \gg R \tag{4}$$

are easy to establish using Fourier series. Thus the error term $E(u)$ in the trapezium rule for a closed curve is well understood. Moreover (3) suggests that if C is sufficiently smooth, then the exponent in (1) should fall, perhaps to $\frac{1}{2} + \varepsilon$.

A related problem, considered by Swinnerton-Dyer [9], is to bound P, the number of lattice points on the curve C. He found the result

$$P \ll R^{3/5+\varepsilon}.$$

The ambiguous status of lattice points on the curve means that

$$D(0,0) \geqslant P/2.$$

Swinnerton-Dyer has suggested that the geometrical ideas in [9] could be applied to the lattice point problem.

Recently Iwaniec and Mozzochi [5], building on previous work by Bombieri and

Iwaniec [1], obtained

$$D(0,0) \ll R^{7/11+\varepsilon}$$

for the circle. Their method can be generalized [3, 4]. In this note we give a strictly elementary proof of (1), taking ideas from [5] and [10] (and thus ultimately from Sierpiński [8]). We use the continued fraction algorithm, which tradition ascribes to Brahmagupta, and the circle method, which first appears in Hardy and Ramanujan's great paper on the partition function [2]. For completeness we also prove (2), (3) and (4) using exponential sums. We hope to shed light on the Iwaniec–Mozzochi memoir, which uses the circle method, exponential sums and the large sieve, and on Jutila's work on Voronoi summation (see for example [6]), which rests on the transformation formula for an Eisenstein series just as Hardy and Ramanujan rely on the transformation formula for the discriminant function. Applying the circle method to exponential sums is a new and exciting development, which may go as far as the circle method for exponential integrals in the hands of Hardy, Littlewood and Vinogradov.

2. The circle method

The circle method in its usual form divides the circle into a large finite number of arcs, each containing a point whose polar angle is $2\pi p/q$ where p and q are small integers. We divide the curve into a large number K of arcs, each of length $\ll L = R/K$, and also of length $\gg L$, and we pick a point on each arc where the tangent has a rational gradient p/q, with p and q numerically as small as possible. We draw the tangent at these points, forming a K-sided polygon circumscribed to the curve. We also draw a polygon with parallel sides inscribed to the curve. Since by assumption the radius of curvature lies between multiples of R, the distance between corresponding sides of the two polygons is $\ll \delta = R/K^2$ and the difference in area of the two polygons is $\ll \delta KL$.

The discrepancy of a polygon is treated in Vinogradov [10], but only through worked examples. There is a contribution from each side and from each vertex: the bound is

$$\ll \sum_k S(\alpha_k, L_k),$$

where the sum is over sides of the polygon, L_k being the side length and α_k its gradient. The sum $S(\alpha, l)$ is defined as follows. Take the continued fraction

$$|\alpha| = a_0 + 1/a_1 + 1/a_2 + \cdots$$

and truncate it at an index r with $q_r \leqslant l$. Then

$$S(\alpha, l) = a_0 + a_1 + \cdots + a_r + l/q_r.$$

We have $L_k \ll L$ for each side k. Since $q_r \ll L$, we have $r \ll \log L$. Fixing $a_0, \ldots, a_{i-1}$ in a continued fraction determines an interval of length Δ say, on which $a_i = n$ for a subinterval of length $\ll \Delta/n^2$. For $|\alpha| \leqslant 1$ the arc on the curve corresponds to an interval of length $\gg 1/K$ within which we must choose a rational number. (For $|\alpha| > 1$

the same argument applies to $1/|\alpha|$). The expectation of a_i is thus

$$\ll \sum_{n \ll L} n \cdot \frac{1}{n^2} \ll \log L$$

independently of $a_0, \ldots, a_{i-1}$. Finally for fixed p_r/q_r there are

$$\ll 1 + K/q_r L$$

tangents for which the truncation of the continued fraction for the gradient p/q gives p_r/q_r. Thus

$$\sum_k S(\alpha_k, L_k) \ll K \log^2 L + \sum_{q \ll L} \left(1 + \frac{K}{qL}\right) \frac{L}{q} \cdot q \ll K \log^2 L + L^2.$$

Since the area of the curve lies between the areas of the circumscribed and inscribed polygons we have

$$D(0,0) \ll \delta K L + K \log^2 L + L^2.$$

Taking

$$K = R^{2/3} (\log R)^{-2/3} + O(1)$$

gives

$$N(0,0) = AR^2 + O(R^{2/3} (\log R)^{4/3}),$$

and the same estimate holds for $N(u, v)$ on translating the curve by the vector (u, v).

3. Fourier analysis of the discrepancy

In this section we use $\sim$ to indicate 'possesses the Fourier series', $\approx$ to indicate 'is asymptotically equal to', and write $e(t)$ for $\exp 2\pi i t$. Since $N(u, v)$ is periodic in u and in v, it has a Fourier series

$$N(u,v) \sim \sum_{h=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} c_{hk} e(hu + kv)$$

with $c_{00} = A$. Writing the 'row of teeth' function as

$$\rho(t) = [t] - t + \tfrac{1}{2} \sim \sum_{k \neq 0} \frac{e(kt)}{2\pi i k},$$

we have

$$N(u,v) = T(u) + \sum_{a-u \leqslant n \leqslant b-u} (\rho(F(n+u) - v)) - \rho(f(n+u) - v)).$$

The second term can be expanded again as

$$\sim \sum_{k\neq 0} \frac{e(-kv)}{2\pi ik} \sum_{a\ u\leqslant n\leqslant b\ u} (e(kF(n+u)) - e(kf(n+u)))$$

$$\sim \sum_{k\neq 0} \frac{e(-kv)}{2\pi ik} \sum_{h} e(hu) \int_0^1 \sum_{a\ x\leqslant n\leqslant b\ x} (e(kF(n+x)) - e(kf(n+x)))e(-hx)\,\mathrm{d}x.$$

Thus for $k \neq 0$

$$2\pi ik\, c_{h,-k} = \int_a^b (e(kF(x) - e(kf(x)))e(-hx)\,\mathrm{d}x = I_1 - I_2,$$

say. Since f'' and $-F''$ are both $\gg 1/R$, van der Corput's second derivative test gives

$$I_1, I_2 \ll (R/|k|)^{1/2}, \quad c_{hk} \ll R^{1/2}/|k|^{3/2}.$$

Similarly we could consider x as a function of y on the curve and obtain

$$c_{hk} \ll R^{1/2}/|h|^{3/2}.$$

Thus

$$|c_{hk}|^2 \ll R/(h^2 + k^2)^{3/2}.$$

Now

$$E(u) \sim \sum_{h\neq 0} c_{h0} e(hu) \ll \sum_{h\neq 0} |c_{h0}| \ll R^{1/2},$$

which gives (2), and by Parseval's identity

$$\int_0^1 |E(u)|^2\,\mathrm{d}u = \sum_{h\neq 0} |c_{h0}|^2 \leqslant \int_0^1 \int_0^1 |D(u,v)|^2\,\mathrm{d}u\,\mathrm{d}v = \sum_{(h,k)\neq(0,0)} \sum |c_{hk}|^2 \ll R,$$

which is (3).

For the lower bound we assume that the curve is three times differentiable. If x_0, x_1 give the maximum of $F(x)$ and the minimum of $f(x)$ respectively, then

$$I_1 \approx \left(\frac{i}{kF''(x_0)}\right)^{\frac{1}{2}} e(kF(x_0)),$$

$$I_2 \approx \left(\frac{i}{kf''(x_1)}\right)^{\frac{1}{2}} e(kf(x_1)),$$

where the square roots of complex numbers are taken with positive real part. If these two integrals cancel, then

$$e(kF(x_0) - kf(x_1)) \approx -i.$$

This approximate equality cannot hold for $k = 1$ and for $k = 2$, so

$$|c_{01}|^2 + |c_{02}|^2 \gg R.$$

By symmetry between the x and y directions, we have

$$|c_{10}|^2 + |c_{20}|^2 \gg R,$$

which gives (4).

References

[1] Bombieri E and Iwaniec H, On the order of $(\frac{1}{2} + it)$, *Ann. Scuola Normale Superiore di Pisa cl. Sci.* (4) **13** (1986) 449–472

[2] Hardy G H and Ramanujan S, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.* 2 **17** (1918) 75–115

[3] Huxley M N and Watt N, Exponential sums and the Riemann zeta function *Proc. London Math. Soc.* (to appear)

[4] Huxley M N, Exponential sums and lattice points (to appear)

[5] Iwaniec H and Mozzochi C J, On the circle and divisor problems (to appear)

[6] Jutila M, *Lectures on a method in the theory of exponential sums* (Bombay: Tata Institute of Fundamental Research) (1987)

[7] Landau E, *Vorlesungen über Zahlentheorie* (Leipzig: Hirzel) Band 2 (1927)

[8] Sierpin'ski W, A certain problem in the calculus of asymptotic functions, *Prace Mat.-Fiz.* **17** (1906) 77–118 and *Oeuvres Choisies* 73–108

[9] Swinnerton-Dyer H P F, The number of lattice points on a convex curve, *J. Number Theory* **6** (1974) 128–135

[10] Vinogradov I M, *An introduction to the theory of numbers* (Oxford: Pergamon) (1955)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 117–155.
© Printed in India.

On the nonvanishing of some L-functions*

HERVÉ JACQUET
Department of Mathematics, Columbia University, New York NY 10027, USA

Abstract. The non-vanishing, at the centre of symmetry, of the L-function attached to an automorphic representation of $GL(2)$ or its twists by quadratic characters has been extensively investigated, in particular by Waldspurger. The purpose of this paper is to outline a new proof of Waldspurger's results. The automorphic representations of $GL(2)$ and its metaplectic cover are compared in two different ways; one way is by means of a "relative trace formula"; the relative trace formula presented here is actually a generalization of the work of Iwaniec.

Keywords. L-function; automorphic representation; relative trace formula; Waldspurger result; metaplectic group.

1. Introduction

(1.1) Let F be a number field, G the group $GL(2)$, regarded as an algebraic group defined over F. Let π be an automorphic representation of G, cuspidal and trivial on the centre of G. Then π is equivalent to its contragredient representation; thus, if η is a quadratic idèle-class character of F, then the L-function attached to $\pi \otimes \eta$ satisfies the functional equation

$$L(s, \pi \otimes \eta) = \varepsilon(s, \pi \otimes \eta) L(1 - s, \pi \otimes \eta).$$

This equation suggests the following question: what are those π for which there is at least one η such that

$$L(\tfrac{1}{2}, \pi \otimes \eta) \neq 0.$$

This question has been studied extensively ([8], [19], [20]). Waldspurger solves this question by using the machinery of the Weil representation. Another approach is to use a "relative trace formula". This approach was first used by Iwaniec ([9] and [10]) and the present paper should be regarded as a mere complement to his work.

(1.2) We first outline the "relative trace formula" in question. Let f be a smooth function on $G(F_A)$, invariant under the centre $Z(F_A)$ and of compact support (modulo the centre). In the usual way f defines a convolution operator $\rho(f)$ on

$$L^2(Z(F_A)G(F)\backslash G(F_A)) \tag{1}$$

which, in turn, is represented by a kernel

$$K[x, y; f] = \sum f(x^{-1}\xi y), \quad \xi \in Z(F)\backslash G(F). \tag{2}$$

---

* This is the text of a lecture delivered in June 1987 in Paris at the Symposium in honour of R Godement. This work was supported in part by NSF grant DMS-85-02789.

We fix a non-trivial character ψ of F_A/F and define, for each η, a distribution $I(f;\eta,\psi)$ by the formula

$$I(f;\eta,\psi)=\int\int K\left[\begin{pmatrix}a&0\\0&1\end{pmatrix},\begin{pmatrix}1&u\\0&1\end{pmatrix}\right]\eta(a)\,\mathrm{d}^{\times}a\psi(-u)\,\mathrm{d}u,$$

$$a\in F_A^{\times}/F^{\times},\quad u\in F_A/F. \tag{3}$$

The integral is absolutely convergent. On the other hand K has a "spectral expression"

$$K(x,y;f)=\sum_{\pi}K_{\pi}(x,y;f)+K_{\mathrm{eis}}(x,y;f). \tag{4}$$

The first sum is over all discrete components of (1). Those are either cuspidal representations or one-dimensional representations of the form:

$$g\mapsto\chi(\det g),\quad \chi^2=1. \tag{5}$$

The kernel K_{eis} represents the contribution of the continuous spectrum. For a given π, the kernel K_{π} is given by a sum:

$$K_{\pi}(x,y;f)=\sum(\rho(f)\varphi_i)(x)\varphi_i(y)^*. \tag{6}$$

(In this paper z^* denotes the imaginary conjugate of z). The sum is over an orthonormal basis of the space of π. When we compute the integral $I(f;\eta,\psi)$ and integrate over the variable u, the contribution of the kernels K_{π} with π one-dimensional is zero. Integrating then over the variable a, we get an expression

$$I(f;\eta,\psi)=\sum_{\pi}I_{\pi}(f;\eta,\psi)+I_{\mathrm{eis}}(f;\eta,\psi) \tag{7}$$

where

$$I_{\pi}(f;\eta,\psi)=\int\int K_{\pi}\left[\begin{pmatrix}a&0\\0&1\end{pmatrix},\begin{pmatrix}1&x\\0&1\end{pmatrix};f\right]\psi(-x)\,\mathrm{d}x\eta(a)\,\mathrm{d}^{\times}a \tag{8}$$

and I_{eis} is defined similarly. Although the integral defining I_{eis} converges as an iterated integral it cannot be interchanged directly with the sums and the integrals which define K_{eis}. In order to do this interchange we use an appropriate "truncation process". The final result is a formula of the form:

$$I_{\mathrm{eis}}(f;\eta,\psi)=I_{\mathrm{cont}}(f;\eta,\psi)+I_{\mathrm{dis}}(f;\eta,\psi). \tag{9}$$

The term I_{cont} is the "continuous part" of I_{eis} and I_{dis} the "discrete part". Altogether then

$$I(f;\eta,\psi)=\sum_{\pi}I_{\pi}(f;\eta,\psi)+I_{\mathrm{dis}}(f;\eta,\psi)+I_{\mathrm{cont}}(f;\eta,\psi). \tag{10}$$

(1.3) On the other hand let G_1 be the group $SL(2,F)$, regarded as an algebraic group defined over F and let $G_1^{\sim}(F_A)$ be the metaplectic cover of $SL(2,F_A)$. There is a non-trivial central extension

$$1\to\{\pm1\}\to G_1^{\sim}(F_A)\to SL(2,F_A)\to 1. \tag{11}$$

The extension splits over $SL(2,F)$ so that we may regard $SL(2,F)$ as a discrete subgroup

of $G_1^{\sim}(F_A)$. A function f' on $G_1^{\sim}(F_A)$ is said to be "genuine" if

$$f'(\dot{y}z) = f'(g)z$$

for $z = \pm 1$.

We only consider "genuine functions", and similarly, "genuine automorphic forms", "genuine representations" of $G_1^{\sim}(F_A)$. Suppose f' is a (genuine) function, smooth of compact support. Then it defines a convolution operator $\rho(f')$ on the genuine part of

$$L^2(SL(2,F)\backslash G_1^{\sim}(F_A)). \tag{12}$$

This operator is defined by a kernel $K(x, y; f')$:

$$K(x, y; f') = \sum f'(x^{-1}\xi y), \quad \xi \in SL(2, F).$$

The extension (11) splits over the group

$$N(F_A) = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, u \in F_A \right\}. \tag{13}$$

Thus we may regard $N(F_A)$ as a subgroup of $G_1^{\sim}(F_A)$. For $\varepsilon \neq 0$ in F we define a distribution $J(f'; \varepsilon, \psi)$ by the formula

$$J(f'; \varepsilon, \psi) = \int\int K\left[\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}; f' \right] \psi(-\tfrac{1}{2}\varepsilon u) \times \psi(-\tfrac{1}{2}\varepsilon v)\, du\, dv, \quad u, v \in F_A/F. \tag{14}$$

As before we have a decomposition of K as

$$K(x, y; f') = \sum K_\sigma(x, y; f') + K_{\text{cis}}(x, y; f'). \tag{15}$$

The sum is over all discrete components σ of the genuine part of (12) and K_{cis} represents the continuous part of the spectrum. Integrating term-wise we get

$$J(f'; \varepsilon, \psi) = \sum_\sigma J_\sigma(f'; \varepsilon, \psi) + J_{\text{cis}}(f'; \varepsilon, \psi). \tag{16}$$

(1.4) The functions f and f' will be products of local functions f_v and f'_v. For each v, f_v is a function on $GL(2, F_v)$, smooth, invariant under the centre, of compact support. The function f'_v is a function on the local metaplectic group $G_1^{\sim}(F_v)$. There is a non-trivial extension

$$1 \to \{\pm 1\} \to G_1^{\sim}(F_v) \to G_1(F_v) \to 1. \tag{17}$$

There will be a finite set of places S, containing all places at infinity, all places of even residual characteristic and all places v where ψ_v, the local component of ψ, has not the ring of integers R_v for conductor. For v not in S the functions f_v and f'_v will be in the Hecke algebras H_v and H'_v respectively. More precisely let K_v be $GL(2, R_v)$; then H_v is the convolution algebra of functions on $GL(2, F_v)$ which are invariant under Z_v, bi-invariant under K_v and compactly supported. Similarly the extension (17) splits over

$$K_{1v} = SL(2, R_v). \tag{18}$$

Thus we may identify K_{1v} with a subgroup K'_v of $G'_1(F_v)$ and H'_v is the convolution algebra of bi-K'_v-invariant functions of compact support. There is an isomorphism

$$H'_v \xrightarrow{\sim} H_v. \tag{19}$$

There is a canonical choice for this isomorphism (§ 2).

(1.5) From now on assume that η belongs to the quadratic extension $F(\sqrt{\varepsilon})\ldots$ Thus if $\eta = 1$, ε must be a square in F. There is a natural geometric condition on f_v and f'_v, the condition of "matching orbital integrals". For a given f_v there is always a f'_v with matching orbital integrals and conversely. Furthermore if f_v and f'_v correspond to one another via the isomorphism (19) then they have matching orbital integrals.

(1.6) Now the distributions $I(f;\eta,\psi)$ and $J(f';\varepsilon,\psi)$ have elementary geometric expressions obtained by integrating directly the expansions for $K(x,y;f)$ and $K(x,y;f')$. If f and f' have matching orbital integrals, that is, if for each v f_v and f'_v have matching orbital integrals then:

$$I(f;\eta,\psi) = J(f';\varepsilon,\psi). \tag{20}$$

To exploit this identity we use the spectral expression for the distributions I and J. Recall that we have fixed a finite set of places S. For $v \notin S$ we take f_v and f'_v to be Hecke functions corresponding to one another by the isomorphism (18). In principle then, the equality (20) should lead to the following identities:

$$I_\pi(f;\eta,\psi) = \sum_\sigma J_\sigma(f';\varepsilon,\psi). \tag{21}$$

The representation π is any cuspidal representation having a vector fixed under K_v for all $v \notin S$. To such a representation is associated, for each v not in S, an algebra homomorphism

$$H_v \to \mathbb{C}. \tag{22}$$

Similarly the representations σ occurring on the right have a K'_v-fixed vector for all v not in S; hence attached to every one of them there is also an algebra homomorphism

$$H'_v \to \mathbb{C}. \tag{23}$$

The representations appearing on the right are all the cuspidal representation for which the homomorphism (23) is identical with the homomorphism (22), modulo the isomorphism $H_v \xrightarrow{\sim} H'_v$. Once this identity is established, one can attack the problem of characterizing those π for which $L(\frac{1}{2}, \pi \otimes \eta)$ is non-zero for at least one η. Unfortunately this requires more information: the relation [6] between the automorphic representations of G'_1 and those of $G^\sim$, (a certain two-fold covering of $GL(2)$), the relation between the automorphic representations of G and $\tilde{G}$ ([3]) and finally the relation between the automorphic forms of G and G_1 ("multiplicity one theorem" for G_1). The last relation is difficult to prove and not available at the moment.

Since whatever we can prove has been established or could be established by the Weil representation method, we chose to simply state and prove our relative trace formula and, in the last section, to sketch the argument giving the characterization, without pretending to be complete.

2. Hecke algebras

(2.1) For the convenience of the reader we will review the structure of the Hecke algebras at hand. Let F be a local non-archimedean field. We denote by $\rho(\chi)$ the representation of $GL(2, F)$ induced by the character

$$\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \mapsto \chi(a)\chi^{-1}(b). \tag{24}$$

Then $\rho(\chi)$ contains a vector fixed under

$$K = GL(2, R), \tag{25}$$

(R is the ring of integers in F) if and only if χ is unramified; calling φ such a K-fixed and x the value of χ on a uniformizer we have, for f in the Hecke algebra H,

$$\rho(\chi)(f)\varphi = f\hat{}(x)\varphi$$

and

$$f \mapsto f\hat{}(x)$$

is an algebra homomorphism of H into $\mathbb{C}$ ("Satake transform"). Any homomorphism of H into $\mathbb{C}$ has this form. Call f_m the characteristic function of

$$Z(F)K\begin{pmatrix} \omega^m & 0 \\ 0 & 1 \end{pmatrix}K,$$

where ω is a uniformizer and $m \geqslant 0$. Then

$$f_0\hat{}(x) \equiv 1$$

and, for $m \geqslant 1$,

$$f_m\hat{}(x) = q^{m/2}(x^m + x^{-m}) + q^{m/2}(1 - q^{-1})\sum x^j,$$
$$-m < j < m, \quad j \equiv 2 \bmod m.$$

(2.2) Let us now describe the group $G_1\tilde{}(F)$ for any local field F. It consists of all pairs

$$(g, z), \quad g \in G_1(F), \quad z = \pm 1,$$

with the multiplication law

$$(g_1, z_1)(g_2, z_2) = (g_1 g_2, z_1 z_2 \alpha(g_1, g_2))$$

where α is a certain cocycle that we now describe. For

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we set

$$x(g) = c \quad \text{if } c \neq 0, \quad = d \quad \text{if } c = 0.$$

On the other hand the Hilbert symbol (a, b) is defined by $(a, b) = 1$ if a has the form $a = x^2 - by^2, (a, b) = -1$ if not.

Then:

$$\alpha(g_1, g_2) = \left(\frac{x(g_1 g_2)}{x(g_1)}, \frac{x(g_1 g_2)}{x(g_2)} \right).$$

If F is non-archimedean and its residual characteristic is odd then α is cohomologically trivial on

$$K_1 = SL(2, R).$$

For our purposes it is more convenient to use a cocycle β cohomologically equivalent to α and identically one on K_1. To that end we define for

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$s(g)$ to be

$$s(g) = (c, d)$$

if $|2|_F = 1$, $dc \neq 0$, and the valuation of c is odd;

$$s(g) = 1$$

in all other cases (in particular if F is archimedean). We then set

$$\beta(g_1, g_2) = \alpha(g_1, g_2) s(g_1) s(g_2) s(g_1, g_2)^{-1}$$

and use β, instead of α to define the multiplication. Then, for $|2|_F = 1$, we have:

$$\beta(k_1, k_2) = 1 \quad \text{for } k_i \in K_1.$$

Thus the map

$$k \mapsto (k, 1)$$

is an isomorphism of K_1 onto a subgroup K' of $G_1^-(F)$.

(2.3) Next we choose a nontrivial character ψ of F and recall the formula

$$\int \Phi\hat{}(x) \psi(\tfrac{1}{2} a x^2) \, dx = |a|^{-1/2} \gamma(a, \psi) \int \Phi(x) \psi(-\tfrac{1}{2} a^{-1} x^2) \, dx, \tag{26}$$

which serves to define the Weil constant γ. Here Φ is a Schwartz-Bruhat function on F and $\Phi\hat{}$ its Fourier transform (defined with respect to ψ):

$$\Phi\hat{}(x) = \int \Phi(y) \psi(yx) \, dy.$$

We set also

$$\mu(a, \psi) = \frac{\gamma(a, \psi)}{\gamma(1, \psi)} (-1, a). \tag{27}$$

Then μ takes its values in the group of complex 4th roots of one and satisfies the following properties

$$\mu(ab, \psi) = \mu(a, \psi)\mu(b, \psi)(a, b), \tag{28}$$

$$\mu(1, \psi) = 1, \tag{29}$$

$$\mu(ab^2, \psi) = \mu(a, \psi), \tag{30}$$

$$\mu(a, \psi)^2 = (-1, a). \tag{31}$$

It follows that any genuine character of the abelian group

$$A_1^{\sim} = \left\{\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, z\right]\right\}$$

has the form

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, z\right] \mapsto \mu(a, \psi) z \chi(a),$$

where χ is a character of F^x. In particular we can define an induced representation $\rho^{\sim}(\chi)$ of $G_1^{\sim}(F)$ by right shifts on the space of functions φ such that

$$\varphi\left[\left[\begin{pmatrix} a & x \\ 0 & a^{-1} \end{pmatrix}, z\right] g\right] = |a| \mu(a, \psi) \chi(a) z \varphi(g).$$

Now suppose $|2|_F = 1$ and R is the conductor of φ. Then

$$\mu(a, \varphi) = 1$$

if the valuation of a is even. The representation $\rho^{\sim}(\chi)$ contains a K' fixed vector, necessarily with multiplicity one, if and only if χ is unramified. Calling φ such a vector and x the value of χ on a uniformizer we have then

$$\rho^{\sim}(\chi)(f')\varphi = f'^{\wedge}(x)\varphi$$

for any f' in the Hecke algebra H'. Then

$$f' \mapsto f'^{\wedge}(x)$$

is an homomorphism from H' to $\mathbb{C}$ and any other homomorphism has this form. In particular define f'_0 by

$$f'_0(g, z) = z \quad \text{if } g \in K_1$$

$$= 0 \quad \text{if not}$$

and, for $m \geq 1$, f'_m by $f'_m(g) = |a|^{-1/2} \mu(a, \varphi)^{-1} z$ if

$$g = \left[k_1 \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} k_2, z\right]$$

with $k_i \in K_1$, and valuation of a equal to $-m$; $f'_m(g) = 0$ if g is not of this form. Then

$$f'^{\wedge}_m(x) = f^{\wedge}_m(x).$$

Since f_m (resp. f'_m) is a basis of H (resp. H') it follows that there is an isomorphism

$$H \to H'$$

taking f_m to f'_m. Equivalently if f goes to f' then

$$f^{\wedge}(x) = f'^{\wedge}(x).$$

We note that this isomorphism depends on the choice of ψ.

3. Computation of $I(f; \eta, \psi)$

(3.1) We now let F be a number field. Let f be a smooth function of compact support on $Z(F_A)\backslash GL(2, F_A)$. We recall the notations $K(x, y; f)$ and $I(f; \eta, \psi)$ from the introduction. Using the Bruhat decomposition and computing formally at first, we get:

$$I(f; \eta, \psi) = S_1(f; \eta, \psi) + S_2(f; \eta, \psi) + \sum H(\xi; f; \eta, \psi), \quad \xi \in F^x, \tag{32}$$

where we have set

$$S_1(f; \eta, \psi) = \int\int f\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right] \eta(a)\, \mathrm{d}^x a \psi(-x)\, \mathrm{d}x, \tag{33}$$

$$S_2(f; \eta, \psi) = \int\int f\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right] \eta(a)\, \mathrm{d}^x a \psi(-x)\, \mathrm{d}x, \tag{34}$$

and

$$H(\xi; f; \eta, \psi) = \int\int f\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right] \eta(a)\, \mathrm{d}^x a \psi(-x)\, \mathrm{d}x, \tag{35}$$

with

$$w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The integrands in (33) and (34) are obviously compactly supported. To see the same is true for (35) and the sum over ξ is actually finite, we establish the following lemma:

Lemma. Let H be a compact set of $GL(2, F_A)$. Then there are compact sets H_1 of F_A^x and H_2 of F_A, a finite set X of F^x such that the relations:

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in HZ(F_A), \quad \xi \in F^x,$$

imply $a \in H_1, x \in H_2, \xi \in X$.

Proof: We may assume H is the product of compact sets H_v with $H_v = GL(2, R_v)$ for

almost all v. It is easy to see that for each v there are constants c_{1v} and c_{2v} such that the relations

$$\begin{pmatrix} a_v & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} 1 & x_v \\ 0 & 1 \end{pmatrix} \in H_v Z_v$$

and

$$y \neq 0.$$

imply that either

$$|x_v| \leqslant 1, \quad |y| \leqslant c_v, \quad c_v^{-1} \leqslant |a_v| \leqslant c_v$$

or

$$1 < |x_v| \leqslant c_v |y|^{-1}, \quad |y| \leqslant c_v, \quad c_v^{-1} \leqslant |a_v| |x_v|^{-2} \leqslant c_v.$$

Furthermore $c_v = 1$ for almost all v. Coming back to the global condition we first find $|\xi|_v \leqslant c_v$, for all v. Thus ξ is in a compact set of the adeles, hence in a finite set X of F^x. On the other hand, the global condition implies that for all v either:

$$|x_v| \leqslant 1 \quad \text{and} \quad c_v^{-1} \leqslant |a_v| \leqslant c_v,$$

or, for some ξ in X;

$$1 < |x_v| \leqslant c_v |\xi|_v^{-1} \quad \text{and} \quad c_v^{-1} \leqslant |a_v| |x_v|^{-2} \leqslant c_v.$$

This already implies that for each v, x_v is in a compact set of F_v and a_v in a compact set of F_v^x. In addition for almost all v we have $c_v = 1$ and $|\xi|_v = 1$ for all ξ in X. Then the relation:

$$1 < |x_v| \leqslant c_v |\xi|_v^{-1}$$

for some ξ in X is actually impossible and we get that, for almost all v:

$$|x_v| \leqslant 1, \quad |a_v| = 1.$$

This proves the lemma.

(3.2) We now consider the spectral expression for the kernel. Recall that

$$I(f;\eta,\psi) = \sum_{\pi} I_{\pi}(f;\eta,\psi) + I_{\text{eis}}(f;\eta,\psi), \tag{36}$$

where the sum is over all cuspidal representations π and (iterated integral):

$$I_{\text{eis}}(f;\eta,\psi) = \int \eta(a)\, \mathrm{d}^x a \int K_{\text{eis}}\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right] \psi(-x)\, \mathrm{d}x. \tag{37}$$

We certainly have

$$I_{\text{eis}} = \lim I(c), \quad c \to +\infty \tag{38}$$

where

$$I(c) = \int_{c^{-1}}^{c} \eta(a)\, \mathrm{d}^x a \int K_{\text{eis}}\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right] \psi(-x)\, \mathrm{d}x, \tag{39}$$

$$c^{-1} \leqslant |a| \leqslant c.$$

(3.3) We now recall the definition of K_{fin}. We fix a subgroup C of $F_A^\times$, isomorphic to $\mathbb{R}_+^\times$, such that $F_A^\times$ is the product of C and F_A^1, the ideles of norm one. All idele class characters are, unless declared otherwise, trivial on C. For each finite place v we set:

$$K_v = GL(2, R_v). \tag{40}$$

If v is infinite real, K_v is the orthogonal group, if v is infinite complex K_v is the unitary group. We call K the product of the K_v and, for each idele class character χ, $V(\chi)$ the space of functions φ on K such that

$$\varphi\left[\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} k\right] = \chi(ab^{-1})\varphi(k), \quad \text{for } \begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \in K. \tag{41}$$

Suppose φ is such a function. More generally, suppose $\varphi(k, u)$ is a function on $K \times \mathbb{C}$, holomorphic or meromorphic in u, such that for each u, $\varphi(\cdot, u)$ is in $V(\chi)$. Then we extend φ into a function $\varphi(g, u, \chi)$ on $G(F_A)$ such that

$$\varphi\left[\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} g, u, \chi\right] = \chi(ab^{-1})|ab^{-1}|^{u+1/2}\varphi(g, u, \chi). \tag{42}$$

The Eisenstein series is defined, for $\operatorname{Re} u > \frac{1}{2}$, by:

$$E(g, \varphi, u, \zeta) = \sum \varphi(\gamma g, u, \chi), \quad \gamma \in A(F)N(F)\backslash G(F) \tag{43}$$

where

$$A = \left\{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}\right\} \quad N = \left\{\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right\}; \tag{44}$$

it continues analytically to the whole complex plane. Its constant term (along N) is defined by

$$\int E(ng, \varphi, u, \chi)\,\mathrm{d}n, \quad n \in N(F)\backslash N(F_A) \tag{45}$$

and is equal to:

$$\varphi(g, u, \chi) + M(u, \chi)\varphi(g, -u, \chi^{-1}), \tag{46}$$

where $M(u, \chi)$ is the intertwining operator from $V(\chi)$ to $V(\chi^{-1})$. We will also need a non-trivial Fourier coefficient:

$$W(g, \varphi, u, \chi) = \int E\left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g, \varphi, u, \chi\right] \psi(x)\,\mathrm{d}x, \quad x \in F_A/F. \tag{47}$$

For each u and χ we may identify $V(\chi)$ with the space of functions on $G(F_A)$ satisfying (42). The group $G(F_A)$ operates then by right shifts and we get a representation of $G(F_A)$ on $V(\chi)$ denoted by $\rho(u, \chi)$. Then $M(u, \chi)$ is an intertwining operator between $\rho(u, \chi)$ and

$\rho(-u, \chi^{-1})$. The kernel K_{eis} is given by the sum

$$\frac{1}{4i\pi}\sum_{\chi}\sum_{j}\int_{-i\infty}^{+i\infty} E[x, \rho(u,\chi)(f)\varphi_j, u, \chi]E[y, \varphi_j, \chi]^* \,\mathrm{d}u. \tag{48}$$

The first sum is over all χ (trivial on C); for each χ the second sum is over an orthonormal basis of $V(\chi)$, made of K-finite vectors. The convergence of the sums and integrals is certainly uniform for x and y in compact sets. From now on, we will assume f to be K-finite. Let P be the group of idele class characters which are unramified at all places, including all places at infinity. Then $V(\chi)$ depends only on the class of χ mod P and we can choose the same basis for all χ in a given class. In each class, the sum on j is then finite and the sum on χ is over finitely many classes mod P.

(3.4) Since $I(c)$ is defined by an integral over a compact set we have

$$I(c) = \frac{1}{4i\pi}\sum_{\chi}\sum_{j}\int_{-i\infty}^{i\infty}\left[\int_{c^{-1}}^{c} E\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \rho(f)\varphi_j, u, \chi\right]\eta(a)\,\mathrm{d}^{\times}a\right] \times W(e, \varphi_j, u, \chi)^* \,\mathrm{d}u. \tag{49}$$

From [11] p. 214, we recall the following expression:

$$\begin{aligned}\int_{c^{-1}}^{c} E\left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \varphi, u, \chi\right]\eta(a)\,\mathrm{d}^{\times}a \\ = L(\tfrac{1}{2}, \eta; \varphi; u, \chi) + \frac{c^{u+1/2}}{u+1/2}[\delta(\chi\eta)\varphi(e) + \delta(\chi^{-1}\eta)\varphi(w)] \\ + \frac{c^{1/2-u}}{1/2-u}[\delta(\chi^{-1}\eta)M(u,\chi)\varphi(e) + \delta(\chi\eta)M(u,\chi)\varphi(w)] + R(c),\end{aligned} \tag{50}$$

where L is the "Mellin transform" of the Eisenstein series (loc. cit.), $R(c)$ a remainder term tending to 0 as c tends to infinity, $\delta(\chi) = 1$ if χ is trivial, $\delta(\chi) = 0$ if not.

In order to use (50) inside the expression (49), we need estimates for the various quantities at hand in terms of u, and for $\chi = \chi_0\chi_1$ with χ_0 fixed an χ_1 in P, in terms of χ_1. Through an oversight, the estimates given in [11] are in terms of u alone, but the proof given in [11] easily extends to give estimates in terms of u and χ_1.

In particular we can substitute (50) in (49) and integrate termwise. As $c \to \infty$, the term containing $R(c)$ tends to 0. Finally we find that I_{eis} is the sum of I_{cont} defined by:

$$I_{\text{cont}}(f; \eta, \psi) = \frac{1}{4i\pi}\sum_{\chi}\sum_{j}\int_{-i\infty}^{i\infty} L(\tfrac{1}{2}, \eta, \rho(u,\chi)(f)\varphi_j, u, \chi)\, W(e, \varphi_j, u, \chi)^* \,\mathrm{d}u \tag{51}$$

and the limit, as $c \to \infty$, of $I_1(c) + I_2(c)$ where

$$I_1(c) = \frac{1}{4i\pi}\sum_{j}\int_{-i\infty}^{i\infty}\frac{c^{u+1/2}}{u+1/2}\mathrm{d}u[\rho(u,\eta)(f)\varphi_j(e) + \rho(u,\eta)(f)\varphi_j(w)] \times W(e, \eta, u, \varphi_j)^* \tag{52}$$

and

$$I_2(c)=\frac{1}{4i\pi}\sum_j\int_{-i\infty}^{i\infty}\frac{c^{1/2-u}}{1/2-u}\,du[\rho(-u,\eta)M(u,\eta)\varphi_j(e)$$
$$+\rho(-u,\eta)M(u,\eta)\varphi_j(w)]\,W(e;\eta,u,\varphi_j)^*. \tag{53}$$

The sum on j is over a basis of $V(\eta)$. We remark that an irreducible K-type τ is contained in $V(\eta)$ with multiplicity atmost one. Thus, on the space of τ, the operator $M(u,\eta)$ must be scalar. This, together with the functional equations for M, E and its Fourier coefficient W, easily imply that I_2 equals I_1. After changing u to $-u$, we see that I_{els} is the sum of I_{cont} and the limit, as $c\to+\infty$, of

$$2I_1(c)=\frac{1}{2i\pi}\sum_j\int_{-i\infty}^{i\infty}\frac{c^{1/2-u}}{1/2-u}[\rho(-u,\eta)(f)\varphi_j(e)$$
$$+\rho(-u,\eta)(f)\varphi_j(w)]W(e;\varphi_j;u,\chi)^*. \tag{54}$$

To compute this integral, we deform the contour of integration. The new contour is the vertical line $\mathrm{Re}(u)=1/2$. We obtain a Cauchy integral over that line plus $-i\pi$ times the residue of the integrand at $1/2$. It is then easy to evaluate the resulting oscillatory integral as $c\to+\infty$. The final result is the term I_{dis} defined by:

$$I_{\text{dis}}(f;\eta,\psi)=-\sum_j[\rho(-\tfrac{1}{2},\eta)(f)\varphi_j(e)$$
$$+\rho(-\tfrac{1}{2},\eta)(f)\varphi_j(w)]W(e;\tfrac{1}{2},\eta;\varphi_j)^*. \tag{55}$$

We remark as before that the various estimates needed for the computation can be extracted from [11]. In particular, $W(g;u,\eta,\varphi_j)$ is holomorphic at $u=\frac{1}{2}$. (loc. cit.)

(3.5) We have now obtained the spectral expression for I:

$$I(f;\eta,\psi)=\sum_\pi I_\pi(f;\eta,\psi)+I_{\text{dis}}(f;\eta,\psi)+I_{\text{cont}}(f;\eta,\psi).$$

4. Local orbital integrals for $GL(2)$

(4.1) In this section F is a number field, ψ a non-trivial character of F, η a character of $F^\times$ whose square is one. Recall the notations:

$$A=\left\{\begin{pmatrix}*&0\\0&*\end{pmatrix}\right\},\quad N=\left\{\begin{pmatrix}1&*\\0&1\end{pmatrix}\right\},$$
$$N^-=\left\{\begin{pmatrix}1&0*&1\end{pmatrix}\right\},\quad w=\left\{\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\}. \tag{56}$$

If f is a smooth function of compact support we set:

$$S_1(f;\eta,\psi)=\int\int f\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}w\begin{pmatrix}1&x\\0&1\end{pmatrix}\right)\eta(a)\,d^\times a\psi(-x)\,dx,$$

$$S_2(f;\eta,\psi)=\int\int f\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}\begin{pmatrix}1&x\\0&1\end{pmatrix}\right)\eta(a)\,\mathrm{d}^{\times}a\psi(-x)\,\mathrm{d}x,$$

and, for y non-zero in F,

$$H(y;f;\eta,\psi)=\int\int f\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}\begin{pmatrix}1&y\\0&1\end{pmatrix}w\begin{pmatrix}1&x\\0&1\end{pmatrix}\right)\eta(a)\,\mathrm{d}^{\times}a\psi(-x)\,\mathrm{d}x.$$

The integrands are clearly compactly supported. We want to study the resulting function of y.

(4.2) PROPOSITION

(i) *There are two functions H_1 and H_2, smooth of compact support on F such that:*

$$H(y;f;\eta,\psi)=H_1(y)+H_2(y)\psi(-y^{-1}). \tag{57}$$

(ii) *If H_1 and H_2 are as in* (57) *then:*

$$H_i(0)=S_i(f;\eta,\psi),\quad i=1,2. \tag{58}$$

(iii) *If H_1 and H_2 are two smooth functions of compact support on F then there is a function f such that relation* (57) *is satisfied.*

(4.3) *Proof of (i)*

Since G is the union of the open sets $NAwN$ and NAN^-, we may assume that the support of f is contained in one of these two open sets. If the support of f is contained in the first set, then the corresponding function H is a smooth function of compact support on F. Moreover, the value of H at zero is S_1. Furthermore, every smooth function of compact support on F is of the form H for an appropriate f with support in the set $NAwN$.

We now assume that the support of the function f is contained in the open set NAN^-. We will show that the corresponding function H has the prescribed form with functions H_1 and H_2 whose values at zero are given by (ii). To that end we introduce:

$$T(u,v)=\int f\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}\begin{pmatrix}1&u\\0&1\end{pmatrix}\begin{pmatrix}1&0\\v&1\end{pmatrix}\right)\eta(a)\,\mathrm{d}^{\times}a. \tag{59}$$

Then T is a smooth function of compact support on $F^{\times}\times F$; in fact, any smooth function of compact support is of this form for an appropriate f. The function H and the quantities S_i attached to f can be written in terms of T as follows:

$$H(y;T)=\int T(x^2y-x,x^{-1})\psi(-x)\,\mathrm{d}x,$$

$$S_1(T)=\int T(-x,x^{-1})\psi(-x)\,\mathrm{d}x$$

$$S_2(T)=\int T(x,0)\psi(-x)\,\mathrm{d}x. \tag{60}$$

Thus the problem at hand is to show that

$$H(y; T) = H_1(y) + H_2(y)\psi(-y^{-1})$$

where H_i is smooth of compact support on F and

$$H_i(0) = S_i(T).$$

Now

$$T(x^2y - x, x^{-1}) \neq 0$$

implies that

$$|x^2y - x| \leqslant C_1, \quad |x^{-1}| \leqslant C_2,$$

where C_1 and C_2 are appropriate constants. These inequalities, in turn, imply that

$$C_2^{-1} \leqslant |x| \leqslant (C_1C_2 + 1)|y|^{-1}, \quad |y| \leqslant C_2(C_1C_2 + 1).$$

This shows that $H(y; T)$ is a smooth function on $F^\times$ which vanishes for $|y|$ large enough. In addition, if the projection of the support of T on the second factor is a compact set of $F^\times$ then it is clear that $H(y; T)$ is smooth at zero as well; furthermore we have then:

$$H(0; T) = S_1(T), \quad S_2(T) = 0.$$

Using the linearity of the problem and a partition of unity we see that it suffices to prove our assertion for a function T whose support is contained in a set of the form:

$$\{(u, v) | |u| \leqslant C_1, |u| \leqslant C_2\},$$

where C_1 is fixed and C_2 can be taken as small as we please. In particular, we may assume $C_1C_2 < 1$; then the support of the integrand in the integral for $S_1(T)$ is empty so that $S_1(T) = 0$. On the other hand, taking $z = x - y^{-1}$ for new variable we find:

$$H(y; T) = \psi(-y^{-1})H_2(y),$$

where

$$H_2(y) = \int T[(1 + yz)z, y(1 + yz)^{-1}]\psi(-z)\,dz. \tag{61}$$

If the integrand is not zero then

$$C_2^{-1}|y| \leqslant |1 + yz| \leqslant C_1|z|^{-1}.$$

In turn, this implies that

$$|yz| \leqslant C_1C_2 < 1,$$

and then:

$$1 - C_1C_2 \leqslant |1 + yz|$$

and finally:

$$|z| \leqslant C_1|1 + yz|^{-1} \leqslant C_1(1 - C_1C_2)^{-1}.$$

Thus the support of the integrand in (60), as a function of z, is contained in a compact set independant of y. Furthermore, for y in a neighbourhood of zero, $1 + yz$ remains in a neighbourhood of one. It easily follows that H_2 is smooth at zero with $H_2(0) = S_2(T)$. This concludes the proof of (57).

(4.4) *Proofs of (ii) and (iii)*

In view of what we have already proved, assertion (ii) amounts to say that if H_1 and H_2 are smooth functions of compact support and

$$H_1(y) + H_2(y)\psi(-y^{-1}) = 0$$

for y small enough, then, in fact,

$$H_1(0) = H_2(0) = 0.$$

This is clear.

We now prove (iii) in the non-archimedean case. Consider an expression of the form:

$$K_1(y) + K_2(y)\psi(-y^{-1}), \tag{62}$$

with K_i smooth of compact support. There is certainly a function f_2, with support in the set NAN^-, such that

$$S_2(f_2; \eta, \psi) = K_2(0).$$

Let us write

$$H(y; f_2; \eta, \psi) = H_1(y) + H_2(y)\psi(-y^{-1}). \tag{63}$$

Then H_2 and K_2 take the same value at 0. Thus the difference between expression (62) and $H(y; f_2; \eta, \psi)$ is a smooth function on F. Thus, it is of the form $H(y; f_1; \eta, \psi)$, with a function f_1 whose support is contained in $NAwN$. Finally (62) has the required form with $f = f_1 + f_2$. Now suppose F is archimedean. Suppose the expression (62) is again given and we can find f_2, with support in the set NAN^-, with the following property: if the function $H(y; f_2; \eta, \psi)$ is written in the form (63) then the functions H_2 and K_2 have the same derivatives at zero. Then the difference between expression (62) and $H(y; f_2; \eta, \psi)$ is again smooth at zero and we can conclude as before.

Recalling the function T introduced before we see that what we have to prove is the following assertion: let T_i, $i = 1, 2$, be smooth functions on F with support in the sets $|u| \leqslant C_i$, $i = 1, 2$, respectively where $C_1 C_2 < 1$. Set

$$H(y) = \int T_1[(1 + yz)z]T_2[y(1 + yz)^{-1}]\psi(-z)\,\mathrm{d}z.$$

Then given a sequence of numbers (a double sequence in the complex case) one can choose T_1 and T_2 in such a way that the derivatives of H at zero are the elements of this sequence. Indeed, as before, we can take the integration over the fixed compact set

$$|z| \leqslant C_1(1 - C_1 C_2)^{-1}$$

which contains the support of T_1. We first choose T_1 in such a way that

$$\int T_1[z]\psi(-z)\,dz = 1.$$

Then $H_2(0) = T_2(0)$ and, in general, the derivatives of H can be computed recursively in terms of the derivatives of T_2 at 0. These relations can be solved for the derivatives of T_2 at 0 and our assertion follows.

5. Orbital integral for $GL(2)$: unramified situation

(5.1) We keep the notations of § 4. In addition, we assume the ground field F is non-archimedean, the conductor of the character ψ is the ring of integers R and the character η is unramified, of square one. We recall the notation of f_m of § 2 the notation ω for a uniformizer and denote by Φ_j the characteristic function of $\omega^j R$ and by Φ^j that of $\omega^j R^\times$. We write $H(y;m)$ for the orbital integral $H(y;f_m;\eta,\psi)$.

PROPOSITION

With the above notations

$$H(y;0) = \Phi^0(y) + \Phi_1(y)[1 + \psi(-y^{-1})]; \tag{64}$$

$$H(y;1) = \eta(\omega)\{\Phi^{-1}(y) + 2\Phi^0(y) + \Phi_1(y)[1 + \psi(-y^{-1})]\} \tag{65}$$

for $m \geqslant 2$

$$H(y;m) = \eta(\omega^m)\{\Phi^{-m}(y) + 2\Phi^{1-m}(y) + \Phi^{2-m}(y)\}. \tag{66}$$

(5.2) *Proof of 5.1: First step*

We introduce an auxiliary integral:

$$I_m(y) = \int f_m\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right)\eta(a)\,d^\times a.$$

To compute $H(y;m)$ we first integrate over a and then over x; the integral over x is broken into an integral over $|x| \leqslant 1$ and an integral over $|x| > 1$. Using the invariance of f_m on the right under K we find:

$$H(y;m) = I_m(y) + \int_{|x|>1} I_m(x^2y - x)\psi(-x)\,dx. \tag{67}$$

On the other hand, I_m is easily computed:

$$I_0 = \Phi_0, \tag{68}$$

$$I_m = \eta(\omega^m)[\Phi_{1-m} + \Phi_{-m}] \quad \text{if } m > 0. \tag{69}$$

(5.3) *Proof of 5.1: Second step*

We need to compute the functions

$$A_j(y) = \int_{|x|>1} \Phi_j(x^2 y - x)\psi(-x)\,dx \tag{70}$$

where $j \leqslant 0$. We first compute A_0. We introduce a new variable $z = x - y^{-1}$. Then:

$$A_0(y) = \psi(-y^{-1}) \int \psi(-z)\,dz, \quad |y| < |1 + yz| \leqslant |z|^{-1}.$$

Thus on the domain of integration we have $|yz| < 1$ and $|1 + yz| = 1$. It follows that the domain of integration can also be defined by the inequalities:

$$|y| < 1 \quad \text{and} \quad |z| \leqslant 1$$

and so

$$A_0(y) = \psi(-y^{-1})\Phi_1(y). \tag{71}$$

(5.4) *Proof of 5.1: Third step*

We now compute A_{-j} for $j \geqslant 1$.

Suppose first $|y| \geqslant 1$. We then introduce as before the new variable z. We obtain:

$$A_{-j}(y) = \int \Phi_{-j}[z(1 + yz)]\psi(-z)\,dz, \quad |y| < |1 + yz|.$$

Since $|y| \geqslant 1$, the domain of integration is simply $|z| > 1$. In particular, on the domain of integration, the ratio of $1 + yz$ to yz is a unit. Thus we find:

$$A_{-j}(y) = \int \Phi_{-j}(yz^2)\psi(-z)\,dz, \quad |z| > 1.$$

This is zero unless $1 \leqslant |y| \leqslant |\omega^{2-j}|$. Then it has the form:

$$A_{-j}(y) = \int \psi(-z)\,dz, \quad 1 < |z| \leqslant C,$$

for some constant C and we find:

$$A_{-j}(y) = -1, \quad \text{for } j \geqslant 1 \text{ and } 1 \leqslant |y| \leqslant |\omega^{2-j}|. \tag{72}$$

Now suppose $|y| < 1$. Then we write A_{-j} as a sum of three integrals A^i, $i = 1, 2, 3$, defined as follows:

$$A^1 = \int_{|xy|>1} \Phi_{-j}(x^2 y - x)\psi(-x)\,dx,$$

$$A^2 = \int_{|xy|=1} \cdots$$

$$A^3 = \int_{|x|>1, |xy|<1} \cdots$$

In the first integrand we have $|x^2y - x| = |x^2y|$. Hence:

$$A^1 = \int \Phi_{-f}(x^2y)\psi(-x)\,dx, \quad |x| > |y^{-1}|.$$

This is a sum of integrals of the form

$$\int \psi(-x)\,dx, \quad |x| = |\omega^{-k}|, \quad k \geqslant 2.$$

Consequently:

$$A^1 = 0. \tag{73}$$

We now compute A^2. Clearly:

$$A^2(y) = \int \Phi_{-f}[y^{-1}(xy-1)]\psi(-x)\,dx, \quad |x| = |y^{-1}|$$

$$= \int \psi(-x)\,dx, \quad |x| = |y^{-1}|, \quad |xy-1| \leqslant |y\omega^{-j}|.$$

Suppose first $|\omega^j| \leqslant |y| < 1$. Then in the above integral the second condition is superfluous and we find:

$$A^2(y) = \int \psi(-x)\,dx, \quad |x| = |y^{-1}|.$$

This is -1 if $|y| = |\omega|$, 0 if $|y| \neq |\omega|$. Suppose now that $|y| < |\omega^j|$. Then the inequality $|xy-1| \leqslant |y\omega^{-j}|$ reads also $|x - y^{-1}| \leqslant |\omega^{-j}|$; it then implies already the equality $|x| = |y^{-1}|$. Thus:

$$A^2(y) = \int \psi(-x)\,dx, \quad |x - y^{-1}| \leqslant |\omega^{-j}|.$$

After changing x to $x + y^{-1}$ we find:

$$A^2(y) = \psi(-y^{-1}) \int \psi(-x)\,dx, \quad |x| \leqslant |\omega^{-j}|,$$

which is zero. Hence we find

$$A^2(y) = -1 \quad \text{if } |y| = |\omega|, \quad = 0 \text{ otherwise.} \tag{74}$$

We now compute A^3. We have

$$A^3(y) = \int \psi(-x)\,dx, \quad 1 < |x| < |y^{-1}|, \quad |x| \leqslant |\omega^{-j}|.$$

If $|y| = |\omega|$, the domain of integration is empty and the integral zero. If $|y| < |\omega|$ then

$$A^3(y) = \int \psi(-x)\,dx, \quad 1 < |x| \leqslant C \quad \text{with} \quad C > 1$$

and we find

$$A^3 = -1.$$

Combining the previous formulae we find at last:

$$A_{-j}(y) = -\Phi_{2-j}(y), \quad \text{if } j > 1. \tag{75}$$

The proof of Proposition 5.1 is now a simple matter of book-keeping: see (67), (68), (69), (70), (71), (72) and (75).

6. Computation of the integral J

(6.1) In this section F is again a number field. For each place v of F we have defined a cocycle β_v on $G_{1v} \times G_{1v}$ with values in $\{+1, -1\}$, as well as a map s_v from G_{1v} to $\{+1, -1\}$. Taking the product of the β_v and the s_v we obtain a cocycle β on $G_1(F_A) \times G_1(F_A)$ and a map s from $G_1(F_A)$ to $\{+1, -1\}$. We define the group $G_1^{\sim}(F_A)$ as the set of all pairs (g, z) with g in $G_1(F_A)$ and z in $\{+1, -1\}$, the product being defined by the rule:

$$(g_1, z_1)(g_2, z_2) = (g_1 g_2, \beta(g_1, g_2) z_1 z_2).$$

We thus have a central extension:

$$1 \to \{+1, -1\} \to G_1^{\sim}(F_A) \to G_1(F_A) \to 1. \tag{76}$$

It splits over $G_1(F)$ and the map r defined by

$$r(\tau) = (\tau, s(\tau))$$

identifies $G_1(F)$ to a subgroup of $G_1(F_A)$. We let f' be a smooth function of compact support on $G_1^{\sim}(F_A)$. As before, we assume f' is genuine and is a product of local genuine functions f'_v. We set:

$$K[(x, y); f'] = \sum_{\xi \in G_1(F)} f'(x^{-1} r(\xi) y). \tag{77}$$

The extension (76) splits also over the subgroup $N(F_A)$ and the map t defined by:

$$t\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right) = \left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, 1\right]$$

identifies $N(F_A)$ to a subgroup of $G_1^{\sim}(F_A)$. The maps r and t coincide on $N(F)$.

We define:

$$J(f'; \varepsilon, \psi) = \int\int K\left[t\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, t\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}; f'\right] \psi(-\varepsilon u/2)\, du\, \psi(\varepsilon v/2)\, dv, \tag{78}$$

both integrals over F_A/F. We also introduce the quantities

$$H(\alpha; f'; \varepsilon, \psi)$$

$$= \int\int f'\left[t\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} r\begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} r(w) t\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right] \psi[\varepsilon(x+y)/2]\, dx\, dy, \tag{79}$$

$$S_1(f';\varepsilon,\psi)=\int f'\left[t\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\right]\psi(\varepsilon x/2)\,\mathrm{d}x, \tag{80}$$

$$S_2(f';\varepsilon,\psi)=\int f'\left[t\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}r\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right]\psi(\varepsilon x/2)\,\mathrm{d}x, \tag{81}$$

all integrals over F_A.

(6.2) Using the Bruhat decomposition we get at once

$$J(f';\varepsilon,\psi)=\sum H(\alpha;f';\varepsilon,\psi)$$
$$+\sum\int\phi\,\mathrm{d}y\int f'\left[t\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}r\begin{pmatrix}\alpha^{-1} & 0\\ 0 & \alpha\end{pmatrix}t\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix}\right]\psi(\varepsilon(x+y)/2)\,\mathrm{d}x. \tag{82}$$

Both sums are over all α non-zero in F. The integral in x is over F_A/F and the integral in y over F_A. Now the integral can also be written in the form:

$$\int\mathrm{d}y\int f'\left[t\begin{pmatrix}1 & x+\alpha^{-2}y\\ 0 & 1\end{pmatrix}r\begin{pmatrix}\alpha^{-1} & 0\\ 0 & \alpha\end{pmatrix}\right]\psi(\varepsilon(x+y)/2)\,\mathrm{d}x.$$

Thus the integral contains as a factor the integral of the character $\psi(y\alpha^2)$ and is thus zero unless $\alpha=1$ or $\alpha=-1$. Finally we have:

$$J(f';\varepsilon,\psi)=\sum_{\alpha\neq 0}H(\alpha;f';\varepsilon,\psi)+S_1(f';\varepsilon,\psi)+S_2(f';\varepsilon,\psi). \tag{83}$$

(6.3) We have also a spectral expression for K:

$$K[x,y;f']=\sum K_\sigma[x,y;f']+K_{\mathrm{eis}}[x,y;f']. \tag{84}$$

The sum is over all isotypic components σ of the discrete spectrum $\grave{o}f\ G_1(F_A)$ on the genuine part of

$$L^2(r(G_1F)\backslash G_1^{\sim}(F_A)).$$

For each σ we choose an orthonormal basis ϕ_j of the corresponding space and then

$$K_\sigma[x,y;f']=\sum_j\rho(f')\phi_j(x)\phi_j(y)^*. \tag{85}$$

We note that the series of the K_σ converges at least in the distribution sense, hence also pointwise, uniformly on compact sets. In particular, a termwise integration on compact sets is certainly justified and we find:

$$J(f';\varepsilon,\psi)=\sum_\sigma J_\sigma(f';\varepsilon,\psi)+J_{\mathrm{eis}}(f';\varepsilon'\psi) \tag{86}$$

where

$$J_\sigma(f';\varepsilon,\psi)=\int\int K_\sigma\left[t\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix},t\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}\right]\psi[\varepsilon(v-u)/2]\,\mathrm{d}u\,\mathrm{d}v, \tag{87}$$

and J_{eis} is defined similarly.

7. Orbital integrals for the metaplectic group

(7.1) In this section F is again a local field. If g is in $G_1(F)$ we will often write g for the element $(g, 1)$ of $\tilde{G_1}(F)$ and $g_1 \cdot g_2$ for the product

$$(g_1, 1)(g_2, 1) = (g_1 g_2, \beta(g_1, g_2)).$$

For a smooth function of compact support f' on $\tilde{G_1}(F)$ we set

$$H(a; f'; \varepsilon, \psi)$$

$$= \int\int f' \left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \cdot w \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \right] \psi(\varepsilon(x+y)/2)\, dx\, dy,$$

$$S_1(f'; \varepsilon, \psi) = \int f' \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right) \psi(\varepsilon x/2)\, dx,$$

$$S_2(f'; \varepsilon, \psi) = \int f' \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right) \psi(\varepsilon x/2)\, dx.$$

The convergence of the integrals will be proved in the next section. We want to study the functions H defined in this way.

(7.2) PROPOSITION

(1) *Given f' there are two smooth functions of compact support H_1 and H_2 on F such that:*

$$H(a; f'; \varepsilon, \psi) = \gamma(\varepsilon a, \psi) |a\varepsilon|^{-1/2} H_1(a) \psi(\varepsilon a^{-1}) + \gamma(-\varepsilon a, \psi) |a\varepsilon|^{-1/2} H_2(a) \psi(-\varepsilon a^{-1}).$$

(2) *If H_1 and H_2 are any two functions of compact support satisfying the above condition then:*

$$H_i(0) = S_i(f'; \varepsilon, \psi).$$

(3) *Given any two smooth functions of compact support H_1 and H_2 on F, there is a smooth function of compact support f' such that relation* (1) *is satisfied.*

(7.3) *Proof of 7.2*

We set

$$A_1 = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Then $G_1(F)$ is the union of the open sets

$$NA_1wN \quad \text{and} \quad NA_1N^-.$$

Thus we may assume that the projection of the support of f' is contained in one of these

sets. If it is contained in the first set, then H is a smooth function of compact support on F^x; furthermore $S_1 = S_2 = 0$. In addition, every smooth function of compact support on F^x is of this form for an appropriate function f' whose support has a projection contained in the first set.

Now suppose the projection of the support of f' is contained in the second set. Then the function T defined by

$$T(a,z) = f'\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}a^{-1} & 0\\ 0 & a\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ z & 1\end{pmatrix}\right)\psi(x)\,dx \tag{88}$$

is a smooth function of compact support on the product $F^x \times F$. So is the function U defined by

$$U(y,a) = T(y, y^{-1}a). \tag{89}$$

In fact, every smooth function of compact support on $F^x \times F$ is of the form U for an appropriate function f. In terms of U we have:

$$H(a) = |a|^{-1}\int U(y,a)(y, ya)\psi[\varepsilon a^{-1}(y + y^{-1})/2]\,dy, \tag{90}$$

$$S_1(f';\varepsilon,\psi) = U(1,0), \tag{91}$$

$$S_2(f';\varepsilon,\psi) = U(-1,0). \tag{92}$$

Integral (90) certainly converges and defines a smooth function on F^x, which vanishes for $|a|$ large. To study the integral near 0 we apply the method of stationary phase to the phase function ϕ defined by:

$$\phi(y) = y + y^{-1}.$$

Its critical points are $+1$ and -1. Using a suitable partition of unity we write:

$$H = K_0 + K_1 + K_2,$$

where K_0 is smooth of compact support on F^x and K_1, K_2 are given by:

$$K_1(a) = |a|^{-1}\int U_1(y,a)\psi[\varepsilon a^{-1}(y + y^{-1})/2]\,dy, \tag{92'}$$

$$K_2(a) = |a|^{-1}(-1,a)\int U_2(y,a)\psi[\varepsilon a^{-1}(y + y^{-1})/2]\,dy; \tag{93}$$

the functions U_i are smooth of compact support on $F^x \times F$; furthermore, the projection of the support of U_1 (resp. U_2) on the first factor is contained in a neighbourhood of 1 in F^{x2} (resp. of -1 in $-F^{x2}$) and

$$U_1(1,0) = U(1,0), \quad U_2(1,0) = U(-1,0).$$

In the integral for K_1 we introduce a new variable given by:

$$y + y^{-1} = 2 + z^2, \quad z = y^{1/2} - y^{-1/2},$$

the square root being defined by the usual binomial expansion. We find then:

$$K_1(a) = \psi(\varepsilon a^{-1})|a|^{-1} \int \Phi_1(z, a)\psi(\varepsilon a^{-1} z^2/2)\,\mathrm{d}z, \tag{93'}$$

where

$$\Phi_1(z, a) = U_1(y, a)|\mathrm{d}y/\mathrm{d}z|,$$

$$\Phi_1(0, 0) = U_1(0, 0)|\mathrm{d}y/\mathrm{d}z|(0) = U_1(0, 0). \tag{94}$$

Then, by definition of the Weil constant, we have:

$$K_1(a) = \psi(\varepsilon a^{-1})|a\varepsilon|^{-1/2}\gamma(\varepsilon a, \psi)H_1(a), \tag{95}$$

where we have set

$$H_1(a) = \int \Phi_1\hat{}\,(-z, a)\psi(-\varepsilon^{-1} a z^2/2)\,\mathrm{d}z, \tag{96}$$

$$\Phi_1\hat{}\,(z, a) = \int \Phi_1\hat{}\,(y, a)\psi(yz)\,\mathrm{d}y.$$

Now H_1 is certainly smooth near 0 and

$$H_1(0) = \int \Phi_1\hat{}\,(-z, 0)\,\mathrm{d}z = \Phi_1(0, 0) = U_1(1, 0) = U(1, 0).$$

Similarly, we have:

$$K_2(a) = \psi(-\varepsilon a^{-1})(-1, a)|a\varepsilon|^{-1/2}\gamma(-\varepsilon a, \psi)H_2(a), \tag{97}$$

where H_2 is smooth near 0 and

$$H_2(0) = U(-1, 0).$$

Thus we have proved proposition 7.2(1) furthermore $H_1(0)$ and $H_2(0)$ have the desired values. Since U is arbitrary $H_1(0)$ and $H_2(0)$ are arbitrary numbers. In the non-archimedean case, the other assertions of § 7.2 are then proved as the corresponding assertions of § 4.2.

To prove the remaining assertions in the archimedean case, we need only show the derivatives of H_1 and H_2 at 0 are arbitrary. Consider H_1 for instance. In formula (96) we have:

$$\Phi_1(z, a) = U_1(y, a)|\mathrm{d}y/\mathrm{d}z|$$

from which we derived the relation

$$H_1(0) = \Phi_1(0, 0) = U_1(1, 0).$$

Assume F is real and let D denote differentiation with respect to a. Then we have:

$$DH_1(a) = \int D\Phi_1\hat{}\,(-z, a)\psi(-\varepsilon^{-1} a z^2/2)\mathrm{d}z$$

$$+ C \int z^2 \Phi_1\hat{}\,(-z, a)\psi(-\varepsilon^{-1} a z^2/2)\,\mathrm{d}z,$$

where C is a constant. For $a=0$ we get:

$$DH_1(0) = \int D\Phi_1^\wedge(-z,0)\,dz + C\int z^2\Phi_1^\wedge(-z,0)\,dz$$
$$= DU_1(1,0) + \cdots.$$

In general, we get a relation of the form:

$$D^jH_1(0) = D^jU_1(1,0) + \text{expression in the } D^kU_1(1,0) \text{ with } k<j.$$

These relations can be solved recursively for the $D^jU_1(1,0)$ in terms of the derivatives of H_1 at 0. It follows that the derivatives of H_1 at 0 are indeed arbitrary and the proof of proposition 7.2 is complete.

(7.4) After a simple algebraic manipulation, we can also write H in the form:

$$H(a;f';\varepsilon,\psi) = |a|^{-1/2}\gamma(a,\psi)(\varepsilon,a)[H_1'(a)\psi(\varepsilon a^{-1}) + H_2'(a)\psi(-\varepsilon a^{-1})], \quad (98)$$

where H_1' and H_2' are smooth of compact support on F and

$$H_1'(0) = S_1(f';\varepsilon,\psi)\gamma(\varepsilon,\psi)\gamma(1,\psi)^{-1}|\varepsilon|^{-1/2}, \quad (99)$$

$$H_2'(0) = S_2(f';\varepsilon,\psi)\gamma(-\varepsilon,\psi)\gamma(1,\psi)^{-1}|\varepsilon|^{-1/2}(-1,-1). \quad (100)$$

We now compare the above result with the one in §4. Suppose η is attached to the quadratic extension $F(\varepsilon^{1/2})$; in other words, suppose $\eta(x)=(\varepsilon,x)$. Let ψ_1 be the character defined by:

$$\psi_1(x) = \psi(-2\varepsilon x).$$

Then we shall say that a smooth function of compact support f on $Z(F)\backslash G(F)$ and a smooth function of compact support f' on $G_1^\sim(F)$ have matching orbital integrals if

$$H(a;f;\eta,\psi_1) = |a|^{1/2}\eta(a)\gamma(a,\psi)^{-1}\psi(\varepsilon a^{-1})H(a;f';\varepsilon,\psi) \quad (101)$$

for all a in F. Comparing our results, we do indeed get:

PROPOSITION

For every function f there is a function f' with matching orbital integrals and conversely.

8. Orbital integrals for the metaplectic group: the unramified situation

(8.1) In this section F is non-archimedean, of odd residual characteristic. We denote by v the normalized valuation on F. The conductor of ψ is the ring of integers R and ε is a unit. We set $\eta(a)=(\varepsilon,a)$ and

$$\psi_1(x) = \psi(-2\varepsilon x).$$

We will prove the following result, where the notations are in §2; as noted in the introduction, this is a mere complement to the papers of Iwaniec.

PROPOSITION

For every $m \geqslant 0$

$$H(a; f_m; \eta, \psi_1) = |a|^{1/2} \eta(a) \gamma(a, \psi)^{-1} \psi(\varepsilon a^{-1}) H(a; f'_m; \varepsilon, \psi).$$

In other words, f_m and f'_m have matching orbital integrals.

(8.2) *Proof of 8.1: First step*

We first introduce, for $m \geqslant 0$, the auxiliary function:

$$I_m(a) = \int f'_m \left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \right] \psi(\varepsilon x/2)\, \mathrm{d}x. \tag{102}$$

If I is a smooth function of compact support on $F^\times$ we also introduce the "Kloosterman integral" attached to I:

$$KI(a) = \int_{|y|>1} I(ay) \psi[\tfrac{1}{2}\varepsilon(y + a^{-2}y^{-1})](y, ya)\, \mathrm{d}y. \tag{103}$$

We will write $H'(a; m)$ for $H(a; f'_m; \varepsilon, \psi)$. To compute $H'(a; m)$ from its definition as given in § 1 we first integrate with respect to y. We break the integral into an integral over $|y| \leqslant 1$ and an integral over $|y| > 1$. The first integral gives I_m because of the invariance of f'_m under the maximal compact. Using the Bruhat decomposition and again the invariance of f'_m under K' we find the second integral is equal to KI_m, that is,

$$H'(a; m) = I_m(a) + KI_m(a). \tag{104}$$

(8.3) *Second step*

Recall the notation Φ_j for the characteristic function of $\omega^j R$ and Φ^j for that of $\omega^j R^\times$. We have at once:

$$I_0 = \Phi^0. \tag{105}$$

Now suppose $m \geqslant 0$. Then:

$$f'_m \left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \right] \neq 0 \tag{106}$$

if and only if

$$\mathrm{Sup}(|a|^{-1}, |xa|, |a|) = |\omega^{-m}|,$$

or, what amounts to the same, one of the following three conditions is satisfied:

$$v(a) = m \quad \text{and} \quad v(x) \geqslant -2m, \tag{107}$$

$$v(a) = -m \quad \text{and} \quad v(x) \geqslant 0, \tag{108}$$

$$v(a) = j \quad \text{with} \quad -m < j < m \quad \text{and} \quad v(ax) = -m. \tag{109}$$

In case (107), the value of f'_m is independant of x and, up to a multiplicative constant, (106) is equal to

$$\int \psi(\varepsilon x/2)\,\mathrm{d}x, \quad v(x) \geqslant -2m,$$

hence is zero. In case (108) f'_m has the constant value

$$|a|^{-1/2}\mu(a,\psi)^{-1},$$

(notations of § 2), hence the integral has the same value. In case (109), we have the following relation in the group G'_1:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{-1} & xa \\ 0 & a \end{pmatrix}$$

and then

$$k_1\cdot\begin{pmatrix} a^{-1} & xa \\ 0 & a \end{pmatrix}\cdot k_2 = \left[\begin{pmatrix} x^{-1}a^{-1} & 0 \\ 0 & xa \end{pmatrix}, (x,-a)\right]$$

where k_1 and k_2 are the following elements of K:

$$k_1 = \begin{pmatrix} x^{-1} & -1 \\ 1 & 0 \end{pmatrix}, \quad k_2 = \begin{pmatrix} 1 & 0 \\ -x^{-1}a^{-2} & 1 \end{pmatrix}.$$

It follows that:

$$I_m(a) = q^{-m/2}\int_{v(xa)=-m} (x,-a)\mu(xa,\psi)^{-1}\psi(\varepsilon x/2)\,\mathrm{d}x, \tag{110}$$

or, recalling the properties of μ:

$$I_m(a) = q^{-m/2}\mu(a,\psi)^{-1}\gamma(1,\psi)\int_{v(xa)=-m} \tau(x,\psi)^{-1}\psi(\varepsilon x/2)\,\mathrm{d}x. \tag{111}$$

With the assumptions we have made, we have:

$$\gamma(1,\psi) = 1, \tag{112}$$

$$\gamma(x,\psi) = 1 \quad \text{if } v(x) \text{ is even}, \tag{113}$$

$$\gamma(x,\psi) = q^{-1/2}\sum \psi(x\omega^{2r}y/2)(y,\omega), \quad y \in R/P, \quad \text{if } v(x) = -2r-1. \tag{114}$$

Thus

$$u \mapsto \tau(xu,\psi)\tau(x,\psi)^{-1}$$

is a character of the group of units whose conductor is either R or P. In particular, (111) is zero, unless the integration is over the set $v(x) = -1$, that is, $v(a) = 1-m$. Then the

integral reduces to a sum over $R^x/1+P$:

$$I_m(a) = q^{-m/2}\mu(a,\psi)^{-1}\gamma(\omega^{-1},\psi)^{-1} \times \sum(x,\omega)\psi(\varepsilon x\omega^{-1}/2)$$
$$= q^{1/2-m/2}\mu(a,\psi)^{-1}(\varepsilon,\omega). \tag{115}$$

We can summarize our results as follows:

Lemma: *We have*:

$$I_0(a) = \Phi^0(a),$$
$$I_m(a) = |a|^{-1/2}\mu(a,\psi)^{-1}[\Phi^{-m}(a) + \eta(\omega)\Phi^{1-m}(a)] \quad \text{if } m \geqslant 1.$$

(8.4) *Third step: Computation of* KI_m *for* $m \geqslant 1$.

Lemma: *For* $m \geqslant 1$ *set*

$$I(a) = |a|^{-1/2}\mu(a,\psi)^{-1}\Phi^{-m}(a). \tag{116}$$

Then KI (*defined by* (103)) *is given by*:

$$KI(a) = |a|^{-1/2}\mu(a,\psi)^{-1}\eta(\omega)\Phi^{1-m}(a). \tag{117}$$

Proof: Replacing I by its definition in (103) and changing y to $a^{-1}y$ we get:

$$KI(a) = |a|^{-1}q^{-m/2}\int (ay,y)\mu(y,\psi)^{-1}\psi[\varepsilon a^{-1}(y+y^{-1})/2]\,\mathrm{d}y,$$
$$|y| > |a|, \quad v(y) = -m. \tag{118}$$

Thus the integral is zero unless $v(a) > -m$. Assume first

$$-m < v(a) \leqslant m.$$

Then in the integrand we have $|\varepsilon a^{-1}y^{-1}| \leqslant 1$ and the integral simplifies to:

$$KI(a) = |a|^{-1}q^{-m/2}\int (ay,y)\mu(y,\psi)^{-1}\psi[\varepsilon a^{-1}y/2]\,\mathrm{d}y, \quad v(y) = -m. \tag{119}$$

This is zero unless $v(a^{-1}y) = -1$ in the integration, that is, $v(a) = 1-m$. Changing back y to ya we get:

$$KI(a) = q^{-m/2}\mu(a,\psi)^{-1}\int \gamma(y,\psi)^{-1}\psi(\varepsilon y/2)\,\mathrm{d}y, \quad v(y) = -1. \tag{120}$$

This can be computed as a sum over $R^x/1+P$:

$$q^{-m/2}\mu(a,\psi)^{-1}\gamma(\omega^{-1},\psi)^{-1}\sum_x \psi(\varepsilon\omega^{-1}x/2)(x,\omega) = q^{1/2-m/2}\mu(a,\psi)^{-1}\eta(\omega). \tag{121}$$

Now assume:

$$v(a) > m.$$

We claim the integral KI is then zero. Indeed suppose $v(a) = m + 2r$ with $r > 0$. Coming back to (118) we set:

$$y = \omega^{-m}x(1+u), \quad u \in P^r, \quad x \in R^x/1 + P^r.$$

Then:

$$y^{-1} = \omega^m x^{-1}(1 - u + u^2 + \cdots)$$

and the integral contains as a factor the integral of

$$\psi[u(\varepsilon a^{-1}\omega^{-m}x - \varepsilon a^{-1}\omega^m x)/2] \tag{122}$$

for u in P^r, which is zero. Suppose now $v(a) = m + 2r + 1$ with $r \geqslant 0$. Then in (118) we set

$$y = \omega^{-m}x(1+u), \quad u \in P^{r+1}, \quad x \in R^x/1 + P^{r+1}.$$

This time the integral contains as a factor the integral of (122) for u in P^{r+1}, which is zero. Our computation of KI is now complete and in agreement with the lemma.

(8.5) *Fourth step: Computation of* $K\Phi^0$

Lemma: We have

$$K\Phi^0(a) = |a|^{-1/2}\eta(a)\mu(a,\psi)^{-1}\Phi(a)[\psi(\varepsilon a^{-1}) + \psi(-\varepsilon a^{-1})].$$

For the sake of completeness we reproduce the proof given in [10]. We have:

$$K\Phi^0(a) = |a|^{-1}\int_{|y|>|a|} \psi(\varepsilon a^{-1}(y + y^{-1})/2]\Phi^0(y)(ay, y)\,\mathrm{d}y. \tag{123}$$

The support of the integrand is empty and the integral zero unless $|a| < 1$. Assume $|a| < 1$. Then we find:

$$K\Phi^0(a) = |a|^{-1}\int_{v(y)=0} \psi[\varepsilon a^{-1}(y + y^{-1})/2](ay, y)\,\mathrm{d}y. \tag{124}$$

Assume first $v(a)$ even:

$$v(a) = 2r, \quad r \geqslant 0. \tag{125}$$

Then $(a, y) = 1$. To compute (124) we set:

$$y = v(1+u), \quad v \in R^x/1 + P^r, \quad u \in P^r.$$

Then:

$$y^{-1} = v^{-1}(1 - u + u^2 + \cdots),$$

and

$$K\Phi^0(a) = |a|^{-1}\sum_v \psi[\varepsilon a^{-1}(v + v^{-1})/2]\int_{P^r} \psi[\varepsilon a^{-1}(v - v^{-1})/2]\,\mathrm{d}u.$$

The inner integral is zero unless

$$v \equiv v^{-1} \bmod P^r,$$

that is

$$v \equiv 1 \quad \text{or} \quad -1 \bmod P^r.$$

Hence, under assumption (125), we find:

$$K\Phi^0(a) = |a|^{-1/2}[\psi(\varepsilon a^{-1}) + \psi(-\varepsilon a^{-1})]. \tag{126}$$

Next assume:

$$v(a) = 1. \tag{127}$$

To compute (124) we set:

$$y = v(1+u), \quad v \in R^x/1+P, \quad u \in P.$$

Then $(a, y) = (\omega, v)$ and we can write (124) as a sum over the multiplicative group of the residual field k of the ground field F; in particular, by passing to the quotient, (ω, v) becomes the unique non-trivial quadratic character ζ of k^x. Thus we find:

$$K\Phi^0(a) = \sum_{v \in k^x} \psi[\varepsilon a^{-1}(v + v^{-1})/2]\zeta(v).$$

This can also be written in the form:

$$K\Phi^0(a) = \sum_{u \in k} \psi[\varepsilon a^{-1}(u/2)] \sum_v \zeta(v),$$

where the sum on v is over all solutions of

$$v + v^{-1} = u.$$

With the usual convention that $\eta(0) = 0$ we have:

$$\sum_{v+v^{-1}=u} \zeta(v) = \zeta(u-2) + \zeta(u+2),$$

and then:

$$K\Phi^0(a) = \sum \psi[\varepsilon a^{-1}u/2]\zeta(u+2) + \sum \psi[\varepsilon a^{-1}u/2]\zeta(u-2),$$

both sums being over k. After changing variables we get

$$K\Phi^0(a) = [\psi(\varepsilon a^{-1}) + \psi(-\varepsilon a^{-1})] \sum_u \psi(\varepsilon a^{-1}u/2)\zeta(u).$$

If we recall the formula for γ (114) and the fact that

$$\gamma(a, \psi) = \mu(a, \psi)^{-1}$$

$$K\Phi^0(a) = |a|^{-1/2}\mu(a,\psi)^{-1}\eta(\omega)[\psi(\varepsilon a^{-1}) + \psi(-\varepsilon a^{-1})]. \tag{128}$$

Finally assume

$$v(a) = 2r+1, \quad r > 0. \tag{129}$$

Then $(a,y) = (\omega,y)$. In (124) we set:

$$y = v(1+u), \quad v \in R^x/1 + P^{r+1}, \quad u \in P^{r+1}.$$

Again:

$$y^{-1} = v^{-1}(1 - u + u^2 + \cdots).$$

Then (124) becomes:

$$K\Phi^0(a) = |a|^{-1}\sum_v \psi[\varepsilon a^{-1}(v+v^{-1})/2](v,\omega)\int_{P^{r+1}}\psi[\varepsilon a^{-1}(v-v^{-1})u/2]\,du.$$

The inner integral is zero unless

$$v \equiv v^{-1} \bmod P^r,$$

that is,

$$v = (1+u) \quad \text{or} \quad -(1+u), \quad \text{with } u \in P^r.$$

Then:

$$v^{-1} = (1 - u + u^2 + \cdots) \quad \text{or} \quad = -(1 - u + u^2 + \cdots),$$

and

$$K\Phi^0(a) = |a|^{-1}q^{-r-1}\sum_v (v,\omega)\sum_u \psi[\varepsilon a^{-1}v(2+u^2)],$$

where the first sum is over v in $\{1,-1\}$ and the second sum over u in P^r/P^{r+1}. Next we change u into $\omega^r u$, the sum being now over R/P. Now we recall the elementary formula

$$\sum \psi[\varepsilon a^{-1}\omega^{2r}u^2/2] = \sum \psi[\varepsilon a^{-1}\omega^{2r}u\omega](u,\omega),$$

the formula for $\tau(a^{-1},\psi)$ [(114)] and, once more, the formula:

$$\gamma(a,\psi) = \mu(a,\psi)^{-1}.$$

We find, under assumption (129),

$$K\Phi^0(a) = |a|^{-1/2}\mu(a,\psi)^{-1}\eta(\omega)[\psi(\varepsilon a^{-1}) + \psi(-\varepsilon a^{-1})]. \tag{130}$$

Finally formulae (126), (128) and (130) can be combined to give the lemma.

(8.6) The proof of Proposition (8.1) is now a simple matter of book-keeping. Formula (104) reduces the computation of $H'(a;m)$ to that of I_m and KI_m; in (8.3) we have computed KI for the functions I appearing in I_m. Thus $H'(a;m)$ can be computed and compared with the results of § 7 to give (8.1).

9. The comparison

(9.1) We let F be a number field, η an idele class character of F of square one, ε an element of F^x such that

$$\eta(a) = (\varepsilon, a). \tag{131}$$

We denote by S a finite set of places containing all places at infinity, all places of even residual characteristic, all places where η ramifies, all places where ε is not a unit and, finally, all places where the conductor of ψ_v is not the ring of integers R_v. We set:

$$\psi_1(x) = \psi(-2\varepsilon x). \tag{132}$$

We consider smooth functions f and f' on $G(F_A)$ and $G_1^{\sim}(F_A)$ respectively; the function f is invariant under the centre. Both functions are compactly supported and products of local functions f_v and f'_v. We assume that for each v the functions f_v and f'_v have matching orbital integrals, that is,

$$\begin{aligned} &H(a_v; f_v; \eta_v, \psi_{1v}) \\ &\quad = |a_v|^{1/2} \eta_v(a_v) \gamma(a_v, \psi_v)^{-1} \psi_v(\varepsilon a_v^{-1}) H(a_v; f'_v; \varepsilon, \psi_v), \end{aligned} \tag{133}$$

for all a_v in the multiplicative group of F_v. For v not in S, we assume that f_v and f'_v are Hecke functions corresponding to one another via the isomorphism described in § 2. The point of § 8 was to prove that these two requirements are compatible.

Theorem: *Under the above assumptions*:

$$I(f; \eta, \psi_1) = J(f'; \varepsilon, \psi).$$

Proof: The proof is a straightforward verification. To begin with

$$H(\alpha; f; \eta, \psi_1) = \Pi_v H(\alpha; f_v; \eta_v, \psi_{1v}), \tag{134}$$

with almost all factors equal to one. Since:

$$t\left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right] r\left[\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}\right] t\left[\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix},$$

with the notations of § 7, we have also for f':

$$H(\alpha; f'; \varepsilon, \psi) = \Pi_v H(\alpha; f'_v; \varepsilon, \psi_v). \tag{135}$$

Now, for a given α, the products

$$|\alpha|_v^{1/2} \eta_v(\alpha) \gamma(\alpha, \psi_v)^{-1} \psi_v(\varepsilon \alpha^{-1})$$

are one for almost all v, while their infinite product, over all v, is one. It follows that:

$$H(\alpha; f; \eta, \psi_1) = H(\alpha; f'; \varepsilon, \psi), \quad \text{for all } \alpha. \tag{136}$$

Next we have:

$$S_i(f; \eta, \psi_1) = \Pi_v S_i(f_v; \eta_v, \psi_{1v}), \tag{137}$$

and (Prop. (4.2)):

$$H(a; f_v, \eta_v, \psi_1) = H_{1v}(a) + H_{2v}(a)\psi_v(2\varepsilon a_v^{-1}), \tag{138}$$

where H_i is a smooth function of compact support and:

$$H_{iv}(0) = S_i(f_v; \eta_v, \psi_{1v}). \tag{139}$$

Similarly:

$$S_i(f'_v; \varepsilon, \psi_v) = \Pi_v S_i(f'_v; \varepsilon, \psi_v) \tag{140}$$

and

$$H(a; f'_v; \varepsilon, \psi_v) = |a|_v^{-1/2}\gamma(a, \psi_v)\eta_v(a) \times [H'_{1v}(a)\psi_v(\varepsilon a^{-1}) + H'_{2v}(a)\psi_v(-\varepsilon a^{-1})], \tag{141}$$

where H'_{1v} and H'_{2v} are smooth functions of compact support on F whose values at zero are given by:

$$H'_{1v}(0) = S_1(f'; \varepsilon, \psi_v)\tau(\varepsilon, \psi_v)\tau(1, \psi_v)^{-1}|\varepsilon|_v^{-1/2},$$
$$H'_{2v}(0) = S_2(f'; \varepsilon, \psi_v)\tau(-\varepsilon, \psi_v)\tau(1, \psi_v)^{-1}|\varepsilon|_v^{-1/2}(-1, -1)_v. \tag{142}$$

From (133), (137) and (138) we get:

$$H_{1v}(0) = H'_{2v}(0), \quad H_{2v}(0) = H'_{1v}(0) \tag{143}$$

and then

$$S_{1v}(f_v; \eta_v, \psi_{1v}) = \gamma(-\varepsilon, \psi_v)\gamma(1, \psi_v)^{-1}|\varepsilon|_v^{-1/2}(-1, -1)_v \times S_{2v}(f'_v; \varepsilon_v, \psi_{1v}),$$
$$S_{2v}(f_v; \eta_v, \psi_{1v}) = \gamma(-\varepsilon, \psi_v)\gamma(1, \psi_v)^{-1}|\varepsilon|_v^{-1/2}S_{2v}(f'_v; \varepsilon_v, \psi_{1v}).$$

Taking the product of these equalities over all v we find again:

$$S_1(f; \eta, \psi_1) = S_2(f'; \varepsilon, \psi),$$
$$S_2(f; \eta, \psi_1) = S_1(f'; \varepsilon, \psi). \tag{144}$$

The theorem follows now from the geometric expressions for I and J (32) and (83).

(9.2) We now compare the spectral expressions for I and J. Since we are merely reproving the results of Waldspurger and would need to use arbitrary functions f, rather than K-finite ones, as we did, we will limit ourselves to a *formal* argument.

Consider a cuspidal representation π of $G(F_A)$, trivial on the centre. The corresponding kernel function K_π is zero unless π contains a non-zero vector fixed under the compact group

$$K^S = \Pi_v K_v, \quad v \text{ not in } S. \tag{145}$$

Denote by H^S the product of the Hecke algebras H_v for v not in S. Let f^S be the tensor product of the functions f_v for v not in S; then f^S is an element of H^S. Furthermore, let f_S be the function equal to the product of the f_v for v in S and the unit element of H_v for v

not in S. Then:

$$K_\pi[x, y; f] = f^S\hat{}(\pi) k_\pi[x, y; f_S], \tag{146}$$

where

$$f^S \mapsto f^S\hat{}(\pi)$$

is the character of the Hecke algebra H^S corresponding to π. In a precise way, for v not in S, we have

$$\pi_v = \pi(\chi_v, \chi_v^{-1})$$

where χ_v is an unramified multiplicative character of F. Let x_v be the value of χ_v on a uniformizer; we have then, with the notations of §2:

$$f^S\hat{}(\pi) = \prod f_v\hat{}(x_v), \quad v \text{ not in } S. \tag{147}$$

Integrating (146) we get:

$$I_\pi(f; \eta, \psi) = f^S\hat{}(\pi) I_\pi(f_S; \eta, \psi_1). \tag{148}$$

There is a similar expression for I_{dis}. Finally, the spectral expression for I can be written as follows:

$$I(f; \eta, \psi_1) = \sum_\pi f^S\hat{}(\pi) I_\pi(f_S; \eta, \psi_1) + f^S\hat{}(\eta \circ \det) I_{\text{dis}}(f_S; \eta, \psi_1)$$
$$+ I_{\text{cont}}(f; \eta, \psi_1). \tag{149}$$

The first two terms constitute an infinite linear combination of characters of the Hecke algebra H^S; distinct representations give rise to distinct characters ("strong multiplicity one"). The last term is a "continuous sum" of characters of H^S. Now suppose there is a ϕ in the space of π such that:

$$\int \phi\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \eta(a)\, d^\times a \neq 0. \tag{150}$$

If π has a K^S-fixed vector, it follows there is f_S such that

$$I(f_S; \eta, \psi_1) \neq 0. \tag{151}$$

Conversely, the non-vanishing of (151) for some f_S implies that (150) is satisfied for some ϕ.

(9.3) We pass to the distribution J. With similar notations, we have:

$$K_\sigma[x, y; f'] = f'^S\hat{}(\sigma) K_\sigma[x, y; f'_S], \tag{152}$$

where

$$f'^S \mapsto f'^S\hat{}(\sigma) \tag{153}$$

denotes the character of H'^S attached to σ. In a precise way, for v not in S, the

representation σ_v has the form

$$\sigma_v = \pi^{\sim}(\chi_v), \tag{154}$$

where χ_v is an unramified character and $\pi^{\sim}(\chi_v)$ is the irreducible component of the representation $\rho^{\sim}(\chi_v)$ (notations of §2) containing the unit representation of K'_v. Let x_v be the value of χ_v on a uniformizer; then

$$f'^{S\wedge}(\sigma) = \Pi f''^{\wedge}(x_v), \quad v \text{ not in } S. \tag{155}$$

Suppose in addition that f'_S is a convolution product $h*h$, where

$$h_1(x) = h(x^{-1})^*. \tag{156}$$

Then K_σ has the form:

$$K_\sigma[x, y; f'_S] = \sum_i \rho(h)\phi_i(x)\cdot\rho(h)\phi_i(y)^*$$

and

$$J_\sigma[f'_S; \varepsilon; \psi] = \sum_i \left| \int \rho(h)\phi_i \left[t\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \right] \psi(\varepsilon u/2)\, du \right|^2.$$

Thus J_σ is a sum of terms positive or zero. It follows that for a given σ with a non-zero K'^S-fixed vector, there is f'_S and ε such that

$$J_\sigma[f'_S; \varepsilon, \psi] > 0,$$

and then the sum, over all σ' attached to the same eigenvalue of H'^S than σ, is also positive. The spectral expression for J reads then:

$$J(f'; \sigma, \psi) = \sum_\sigma f'^{S\wedge}(\sigma) J_\sigma(f'_S; \varepsilon, \psi) + J_{\text{cont}}(f'; \sigma, \psi). \tag{156'}$$

(9.4) Using the usual argument on the infinite linear independance of characters, we see that under the assumptions of Theorem (9.1):

$$I_{\text{cont}} = J_{\text{cont}} \tag{157}$$

and, for each π,

$$I_\pi(f_S; \pi, \psi_1) = \sum_\sigma J_\sigma(f'_S; \varepsilon, \psi), \tag{158}$$

the sum over all ε such that

$$f'^{S\wedge}(\pi) = f'^{S\wedge}(\pi). \tag{159}$$

Similarly, we have:

$$I_{\text{dis}}(f_S; \eta, \psi_1) = \sum_\sigma J_\sigma(f'_S; \pi, \psi), \tag{160}$$

the sum over all σ such that:

$$f'^{S\wedge}(\eta\circ\det) = f'^{S\wedge}(\sigma). \tag{161}$$

To begin with the representations σ appearing in (161) are "Weil components", that is, irreducible components of some Weil representation (for a quadratic form in one variable). They will not be mentioned again, although (161) could perhaps be used to some profit. Next, if π satisfies (150) then it has a non-zero K^S-fixed vector, for S large enough; take ε as in (131). Then by (158) there is a σ satisfying (159); more precisely, there is ϕ in the space of σ such that:

$$\int \phi\left[t\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\right]\psi(-\varepsilon u/2)\,\mathrm{d}u \neq 0. \tag{162}$$

Conversely, let π be given. Assume there is S and σ satisfying (159). Then there is f'_S and π such that the right hand side of (158) is positive. It follows that the left hand side is positive and (150) is verified with η defined by (131).

In summary, we see there is a character η such that

$$L(1/2, \pi \otimes \eta) \neq 0 \quad \text{and} \quad \eta^2 = 1 \tag{163}$$

if and only if there is σ satisfying relation (159), for a large enough S. In other words, the existence of a character satisfying (163) is equivalent to the existence of a set S, a representation σ and, for each v not in S, a character χ_v unramified such that

$$\pi_v = \pi(\chi_v, \chi_v^{-1}) \quad \text{and} \quad \sigma_v = \pi^{\sim}(\chi_v).$$

This is the main qualitative result of Waldspurger.

10. Conclusion

(10.1) Finally, we come to the characterization of the representations π for which there is η such that

$$L(1/2, \pi \otimes \eta) \neq 0, \quad \eta^2 = 1. \tag{164}$$

This is the result of Waldspurger (see [17], [6]). It is based on the previous results and the relation, established by Flicker [3], between the representations of $G = GL(2)$ and its two-fold covering $G^{\sim}$. One needs also extra information on the relation between the representations of $G_1^{\sim}$ and those of $G^{\sim}$ as explained in [6]. Another approach is to use a property of the representations of $GL(2)$ whose importance was pointed out in [16]; Langlands also remarked this property should follow from the conjectural relation between the representations of $SL(2)$ and $PGL(3)$, a question later considered by Flicker. At any rate, we state this property as a hypothesis and sketch a proof of the characterization, assuming the hypothesis.

Hypothesis: Let π_1 and π_2 be cuspidal representations of $GL(2, F_A)$ with the same central character. Suppose there is a finite set of places S and, for each v not in S, a character η_v such that

$$\eta_v^2 = 1, \quad \pi_{1v} = \pi_{2v} \otimes \eta_v.$$

Then there is an idele class character η such that

$$\eta^2 = 1 \quad \textit{and} \quad \pi_1 = \pi_2 \otimes \eta.$$

Recall the group $G^{\sim}(F_A)$ is a two-fold covering of $G(F_A)$, and for each place v, the group $G_v^{\sim}$ is a two-fold covering of G_v containing $G_{1v}^{\sim}$. The group $G(F)$ may be regarded as a subgroup of $G^{\sim}(F_A)$.

The group $G_1^{\sim}(F_A)$ (resp. $G_{1v}^{\sim}$) is the subgroup of elements of $G^{\sim}(F_A)$ which project onto some element of $G_1(F_A)$ (resp. G_{1v}). Now consider a finite place v of odd residual characteristic. Then the group $G_v^{\sim}$ contains a subgroup $K_v^{\sim}$ isomorphic to K_v. Consider the representation of $G_v^{\sim}$ induced by the character

$$\left[\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}, z\right] \mapsto \mu(a,\psi)\nu(a)\nu'(b)z. \tag{165}$$

Its class depends only on the square of ν and ν' and will be denoted by $\rho^{\sim}(\nu^2, \nu'^2)$. The restriction of this representation to $G_{1v}^{\sim}$ decomposes into the direct sum of the representations $\rho^{\sim}(\chi)$, where χ is any character such that

$$\chi^2 = \nu^2\nu'^{-2}. \tag{166}$$

In particular, $\rho^{\sim}(\nu^2, \nu'^2)$ contains the unit representation of K_v' if and only if $\nu^2\nu^{-2}$ is unramified and there are then two unramified characters χ satisfying (166). Furthermore, $\rho^{\sim}(\nu^2, \nu'^2)$ contains the unit representation of $K_v^{\sim}$, the maximal compact subgroup of $G_v^{\sim}$, if and only if ν^2 and ν'^2 are unramified; the multiplicity is then one and we denote by $\pi^{\sim}(\nu^2, \nu'^2)$ the irreducible component containing the unit representation of $K_v^{\sim}$.

The fundamental result of [3] is that given a genuine irreducible representation $\pi^{\sim}$ of $G^{\sim}(F^A)$ contained in the cuspidal spectrum but not in the "Weil spectrum" then there is an automorphic cuspidal representation π of $G(F_A)$ whose central character is a square, a finite set of places S containing all even and infinite places, for each place v in S, unramified characters χ_{1v} and χ_{2v} such that

$$\pi_v = \pi(\chi_{1v}, \chi_{2v}), \quad \pi_v^{\sim} = \pi^{\sim}(\chi_{1v}, \chi_{2v}). \tag{167}$$

Furthermore, if π is a given cuspidal representation of $G(F_A)$, whose central character is a square, then there is a representation $\pi^{\sim}$ and a set S satisfying the above condition if and only if the following condition is satisfied: at every place v where π_v has the form:

$$\pi_v = \pi(\mu_{1v}, \mu_{2v}) \quad \text{we have } \mu_{1v}(-1) = \mu_{2v}(-1) = 1. \tag{168}$$

(10.2) Now we can state the following criteria (assuming the hypothesis (10.1)):

PROPOSITION

Let π be a cuspidal representation of $GL(2, F_A)$ with trivial central character. The following conditions are equivalent:

(i) *There is a character η such that*

$$L(1/2, \pi \otimes \eta) \neq 0 \quad \textit{and} \quad \eta^2 = 1.$$

(ii) *Let T be the set of places where π_v is in the discrete series (i.e. not of the form (168)).*

Then there is a character ω of the idele class group such that, for v not in T,

$$\varepsilon(1/2, \pi_v, \psi_v) = \omega_v(-1).$$

Proof: Suppose π satisfies (i). Then there is a cuspidal representation σ_1 of $G_1^{\sim}(F_A)$, a finite set of places S containing all even and infinite places, and, for each v not in S, an unramified character χ_v such that

$$\pi_v = \pi(\chi_v, \chi_v^{-1}), \quad \sigma_{1v} = \pi^{\sim}(\chi_v). \tag{169}$$

Now σ_1 is contained in a cuspidal representation σ of $G^{\sim}(F_A)$. At the cost of enlarging S, we may assume that, for each v not in S, there are unramified characters χ_{1v} and χ_{2v} such that

$$\sigma_v = \pi^{\sim}(\chi_{1v}, \chi_{2v}). \tag{170}$$

Then:

$$\chi_v = \chi_{1v}\chi_{2v}^{-1}. \tag{171}$$

Let π' be the representation of $G(F_A)$ attached to σ by [3]. Its central character is the square of a character ω. For v not in S, we have:

$$\pi'_v = \pi(\chi_{1v}, \chi_{2v}). \tag{172}$$

Thus there is a character ζ_v of square one such that

$$\pi_v = \pi'_v \otimes \omega_v^{-1} \otimes \zeta_v. \tag{173}$$

By the hypothesis, there is an idele class character η of square one such that:

$$\pi = \pi' \otimes \omega^{-1} \otimes \eta. \tag{174}$$

For v not in T, we have:

$$\pi_v = \pi(\mu_v, \mu_v^{-1}). \tag{175}$$

Hence:

$$\pi'_v = \pi(\mu_v\omega_v\eta_v, \mu_v^{-1}\omega_v\eta_v), \tag{176}$$

and by (168)

$$\mu_v(-1) = \omega_v\eta_v(-1). \tag{177}$$

Since for such a v we have:

$$\varepsilon(1/2, \pi_v\psi_v) = \varepsilon(1/2, \mu_v, \psi_v)\varepsilon(1/2, \mu_v^{-1}, \psi_v) = \mu_v(-1), \tag{178}$$

we arrive at condition (ii). Now suppose (ii) is satisfied. Let π' be $\pi \otimes \omega$. Then for v not in T we have:

$$\pi'_v = \pi(\mu_v\omega_v, \mu_v^{-1}\omega_v) \tag{179}$$

with

$$\mu_v\omega_v(-1) = \mu_v^{-1}\omega_v(-1) = 1. \tag{180}$$

Hence there is a representation σ' of $G^{\sim}(F_A)$, a finite set of places S containing T, the

infinite places, the even places, the places where ω or π ramify such that, for v not in S,

$$\sigma'_v = \pi^{\sim}(\mu_v \omega_v, \mu_v^{-1}\omega_v). \tag{181}$$

Let σ_1 be a cuspidal representation of $G^{\sim}(F_A)$ contained in σ'. Then, for v not in S, there is an unramified character χ_v such that

$$\sigma_{1v} = \pi^{\sim}(\chi_v) \quad \text{and} \quad \chi_v^2 = \mu_v^2. \tag{182}$$

Next, by the results of § 8, there is a cuspidal representation π_1 of $G(F_A)$, with trivial central character, such that for v not in S,

$$\pi_{1v} = \pi(\chi_v, \chi_v^{-1}). \tag{183}$$

Furthermore, there is a character η satisfying (i) for the representation π_1. Finally, just as before, there is η_1 of square one such that $\pi = \pi_1 \otimes \eta_1$ and condition (i) is thus satisfied by the representation π.

(10.3) To put condition (ii) into more transparent form, we make the following remark:

Suppose $a_v = 1$ or -1 is given for every place v, with $a_v = 1$ for almost all v. Then there is an idele class character ω such that $\omega_v(-1) = a_v$ for all v if and only if we have:

$$\Pi_v a_v = 1.$$

Now in (10.2) we have, for all v,

$$\varepsilon(1/2, \pi_v, \psi_v) = 1 \quad \text{or} \quad -1.$$

Thus, if T is empty, condition (ii) amounts to

$$\varepsilon(1/2, \pi) = \Pi_v \varepsilon(1/2, \pi_v, \psi_v) = 1.$$

On the other hand, if T is not empty, then condition (ii) is always satisfied.

(10.4) *Remark*

It T is empty then for any quadratic character η we have:

$$\varepsilon(1/2, \pi_v \otimes \eta_v, \psi_v) = \varepsilon(1/2, \pi_v, \psi_v) \quad \text{for any } v,$$

hence:

$$\varepsilon(1/2, \pi \otimes \eta) = \varepsilon(1/2, \pi).$$

References

[1] Bruggeman R, Fourier coefficients of cusps forms, *Invent. Math.* **45** (1978) 1–18

[2] Deshouillers J M and Iwaniec H, Kloosterman sums and Fourier coefficients of cusp forms, *Invent. Math.* **70** (1982) 219–288

[3] Flicker Y, Automorphic forms on covering groups of $GL(2)$, *Invent. Math.* **57** (1980) 119–182

[4] Flicker Y and Kazdhan D, Metaplectic correspondence, *Publ. Math. IHES* No. 64 (1986) pp. 53–110

[5] Gelbart S, Weil's representations and the spectrum of the metaplectic group, *Lecture notes in Mathematics* (Heidelberg, Berlin, New York: Springer-Verlag) vol. 530 (1976)

[6] Gelbart S and Piatetski Shapiro I, Some remarks on metaplectic cusp forms and the correspondences of Shimura and Waldspurger, *Isr. J. Math.* **44** (1983) 97–126
[7] Gelbart S and Soudry D, On Whittaker models and the vanishing of Fourier coefficients of cusp forms *Proc. Indian Acad. Sci. (Math. Sci.)* **97** (1987) 67–74
[8] Goldfeld D, Hoffstein D and Patterson J, On automorphic functions of half-integral weight with applications to elliptic curves, in: *Number theory related to Fermat's last theorem* (Boston: Birkhauser) (1982) pp. 153–193
[9] Iwaniec H, On Waldspurger theorem (preprint)
[10] Iwaniec H, Fourier coefficients of modular forms of half-integral weight, *Invent. Math.* **87** (1987) 385–401
[11] Jacquet H, Sur un résultat de Waldspurger, *Ann. Scient. Ec. Norm. Sup.* 4'Series, t **19** (1986) 185–229
[12] Kazdhan D and Patterson S, Metaplectic forms, *Publ. Math.* No. 59 (1982) 35–142
[13] Kazdhan D and Patterson S, Towards a generalized Shimura correspondence, *Adv. Math.* **60** (1986) 161–234
[14] Kuznietsov N V, Peterson hypothesis for parabolic forms of weight zero and Llinnik hypothesis, *Math. Sborn.* **111** (1980) 334–383
[15] Kohnen W, Fourier coefficients of modular forms of half integral weight, *Math. Ann.* **271** (1985) 237–268
[16] Labesse J-P and Langlands R, *L*-indistinguishability for *SL*(2), *Can. J. Math.* **31** (1979) 726 – 785
[17] Piatetski Shapiro I, Work of Waldspurger, in: *Lie group representations II, Lecture notes in mathematics* (Springer-Verlag) vol. 1041 (1984) pp. 280–301
[18] Salié H, Uber die Kloostermannschen summen $S(u, r; q)$, *Math. Z.* **34** (1931) 91–109
[19] Waldspurger J-L, Correspondence de Shimura, *J. Math. Pure Appl.* **59** (1980) 1–113
[20] Waldspurger J-L, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pure Appl.* **60** (1981) 375–484

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 157–166.
© Printed in India.

On exponential sums involving the Ramanujan function

M JUTILA
Department of Mathematics, University of Turku, SF-20500, Turku, Finland

Abstract. Let $\tau(n)$ be the arithmetical function of Ramanujan, α any real number, and $x \geqslant 2$. The uniform estimate

$$\sum_{n \leqslant x} \tau(n) e(n\alpha) \ll x^6 \log x$$

is a classical result of J R Wilton. It is well known that the best possible bound would be $\ll x^6$. The validity of this hypothesis is proved.

Keywords. Exponential sums; Ramanujan τ function.

1. Introduction

The Ramanujan function $\tau(n)$, usually defined by the identity

$$x \prod_{m=1}^{\infty} (1 - x^m)^{24} = \sum_{n=1}^{\infty} \tau(n) x^n \quad (|x| < 1),$$

also appears in the Fourier series

$$\Delta(z) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e(nz) \quad (\operatorname{Im} z > 0)$$

of the discriminant $\Delta(z)$, which is a cusp form of weight 12 for the full modular group ([1], Theorems 1.19, 3.2 and 3.3). The latter property implies, after Hecke, an analytic continuation and a functional equation for the generating Dirichlet series of $\tau(n)$. The functional equation, in turn, implies a formula of the Voronoi type for the sum function of $\tau(n)$. More generally, a formula for the exponential sum

$$A(x, \alpha) = \sum_{n \leqslant x}{}' \tau(n) e(n\alpha),$$

where $\alpha = h/k$ is a rational number and the summation convention $\sum'$ is as in [4], can be proved in the same way. The result is as follows ([4], Theorem 1.6):

$$A(x, h/k) = x^6 \sum_{n=1}^{\infty} \tau(n) e_k(-n\bar{h}) n^{-6} J_{12}(4\pi\sqrt{nx}/k), \tag{1}$$

where $e_k(x) = e(x/k) = \exp(2\pi i x/k)$, $h\bar{h} \equiv 1 \pmod{k}$, and $J_{12}(x)$ is a Bessel function in the standard notation.

Two approximate variants of (1) may be noted. First, on applying the well-known asymptotic formula for $J_{12}(x)$ and the mean value theorem

$$\sum_{n\leqslant x}\tau^2(n) = Ax^{12} + O(x^{12-2/5}) \tag{2}$$

due to R A Rankin [7], we obtain

$$A(x,h/k) = (\pi\sqrt{2})^{-1}k^{1/2}x^{23/4}\sum_{n=1}^{\infty}\tilde{\tau}(n)e_k(-n\bar{h})n^{-3/4}$$
$$\times\cos(4\pi\sqrt{nx}/k-\pi/4)+O(k^{3/2}x^{21/4}), \tag{3}$$

where $\tilde{\tau}(n)=\tau(n)n^{-11/2}$ is the "normalized" Ramanujan function. By (2), $\tilde{\tau}(n)$ is bounded on the average. It was conjectured by S Ramanujan and proved by P Deligne [2] that $|\tilde{\tau}(n)|\leqslant d(n)$, where $d(n)$ is the usual divisor function. As a truncated version of (3), we have ([4], Theorem 1.1)

$$A(x,h/k) = (\pi\sqrt{2})^{-1}k^{1/2}x^{23/4}\sum_{n\leqslant N}\tilde{\tau}(n)e_k(-n\bar{h})n^{-3/4}$$
$$\times\cos(4\pi\sqrt{nx}/k-\pi/4)+O(kx^{6+\varepsilon}N^{-1/2}), \tag{4}$$

where $k\leqslant x, 1\leqslant N\ll x$, and ε is an arbitrarily fixed small positive number. If N is appropriately chosen and the sum on the right is estimated by absolute values, then it follows that (see (1.5.21) in [4])

$$A(x,h/k)\ll k^{2/3}x^{6-1/6+\varepsilon}. \tag{5}$$

But sometimes it is possible to make use of cancellation in the sum to prove more refined estimates; such a result is given in Lemma 2 below.

The problem of the order of $A(x,\alpha)$ is more difficult if α is not a rational number with a small denominator (in comparison with x). It was proved by J R Wilton [8] that

$$A(x,\alpha)\ll x^6\log x \tag{6}$$

uniformly in α. This is not far from being best possible, for the mean square of $A(x,\alpha)$ with respect to α over the interval $[0,1]$ is of the order Ax^{12} by (2), so that the right hand side of (6) cannot be replaced by anything of a smaller order than x^6. It was conjectured by L A Parson and M Sheingorn [6] that the factor $\log x$ can in fact be removed from (6). It is our object in this paper to prove this conjecture.

Theorem *We have*

$$A(x,\alpha)\ll x^6, \tag{7}$$

uniformly for all real α *and* $x\geqslant 1$.

It will be more convenient to deal with a segment

$$A(x_1,x;\alpha) = A(x,\alpha)-A(x_1,\alpha)$$

of the sum $A(x,\alpha)$ instead of the complete sum itself. We denote by $\tilde{A}(x,\alpha)$ and

$\tilde{A}(x_1, x; \alpha)$ similar sums in which $\tau(n)$ is replaced by $\tilde{\tau}(n)$. Obviously it suffices to prove that

$$A(x_1, x; \alpha) \ll x^6 \tag{8}$$

for $x/2 \leqslant x_1 < x$, or equivalently, that

$$\tilde{A}(x_1, x; \alpha) \ll x^{1/2}. \tag{9}$$

Our arguments will be similar to those in [3], with some refinements. In [3] we studied sums involving $d(n)$, but from the point of view of methods this does not make an essential difference, for the respective summation formulae involving $d(n)$ or $\tau(n)$ are analogous (see [4], Theorem 1.7). Moreover, in place of $\tau(n)$ we might have the Fourier coefficients of any cusp form; if κ is the weight of the form, then $x^{\kappa/2}$ should stand on the right of (7). But for simplicity we work with the Ramanujan function.

A natural approach to the assertion (9) is to write a rational approximation

$$\alpha = h/k + \eta \tag{10}$$

to our number α and to make use of our knowledge about $A(x, h/k)$. Given a number $K \geqslant 1$, we take h/k from the Farey sequence of the order K, in other words

$$(h, k) = 1, \quad k \leqslant K, \quad |\eta| \leqslant (kK)^{-1}. \tag{11}$$

We shall choose $K = x^{1/4}$, and consider separately the cases

$$k^2\eta^2 x \leqslant 1/2 \tag{12}$$

and

$$k^2\eta^2 x \gg 1. \tag{13}$$

The case (12) is easier, for then η is relatively small, and therefore it is possible to make effective use of partial summation and estimates for $A(x, h/k)$.

The case (13) is more delicate. The crucial relation in our proof of (9) is the approximate functional equation

$$\frac{\tilde{A}(x_1, x; \alpha)}{x^{1/2}} = \frac{\tilde{A}(y_1, y; \beta)}{y^{1/2}} + O(y^{-a}), \tag{14}$$

where

$$y_1 = k^2\eta^2 x_1, \quad y = k^2\eta^2 x, \tag{15}$$

$$\beta = -\bar{h}/k - (k^2\eta)^{-1}, \tag{16}$$

and a is a positive constant. An analogous relation for exponential sums involving $d(n)$ was obtained in [3], with the weaker error term $O(\log x)$ however.

Now it is easy to deduce (9) from (14) by an iterative argument. Indeed, we have $y \leqslant K^{-2}x = x^{1/2}$, so that the length of the sum is considerably reduced at each step of the iteration. We stop if we come to a sum for which either (12) holds *mutatis mutandis*, or whose length is $O(1)$. In any case, the last quotient, say $\tilde{A}(z_1, z; \gamma)/z^{1/2}$, is bounded. Then, since the sum of the error terms appearing in the course of the

iteration procedure is bounded as well, we find that the quotient on the left of (14) is bounded. Hence (9) holds.

2. Lemmas on exponential sums and integrals

We first quote from [5], § 1.6, a general estimate for exponential sums of the type

$$S = \sum_{M}^{M'} \tilde{\tau}(m) g(m) e(f(m)).$$

(Actually the result in [5] is given for a similar sum in which $d(m)$ stands in place of $\tilde{\tau}(m)$, but the same method applies in both cases.) To formulate the lemma, define for a real interval $[a, b]$ and for $\mu > 0$ the complex domain

$$D(a, b; \mu) = \{z : |z - x| < \mu \text{ for some } x \in [a, b]\}.$$

We write $A \asymp B$ to mean that $A \ll B \ll A$.

Lemma 1. Let $2 \leqslant M < M' \leqslant 2M$, and let f be a holomorphic function in the domain $D = D(M, M'; \mu)$, where $\mu \asymp M$. Suppose that $f(x)$ is real for $M \leqslant x \leqslant M'$, and that for a certain positive number $F \gg M$ we have

$$f'(z) \ll FM^{-1} \quad \text{for} \quad z \in D,$$

$$|f''(x)| \asymp FM^{-2} \quad \text{for} \quad M \leqslant x \leqslant M'.$$

Let g be a continuously differentiable function in the interval $[M, M']$, where $g(x) \ll G$ and $g'(x) \ll G'$. Then

$$S \ll (G + (M' - M)G')M^{1/2}F^{1/3+\varepsilon}.$$

Remark. An exponential sum of the type

$$S' = \sum_{M}^{M'} \tilde{\tau}(m) g(m) e(f(m) + \theta m),$$

where f and g satisfy the above conditions, occurs in the proof of the next lemma. We may suppose that $|\theta| \leqslant 1/2$. Hence if $M \ll F$, then Lemma 1 can be applied with $f(z) + \theta z$ in place of $f(z)$. In addition to this, we need an estimate for S' in the case $F \ll M \ll F^{1+d}$, where d is a small positive constant. The method in [5], § 4.2, works for S' as well and yields an estimate which is at most by a small power of F (depending on d) weaker than the corresponding estimate for S in Lemma 1.

Lemma 2. For $x \geqslant 1$ and $k \ll x^{1/4}$ we have

$$\tilde{A}(x, h/k) \ll k^{1/4}x^{3/8+\varepsilon} + \min(k^2x^{\varepsilon}, x^{1/2-c}), \tag{17}$$

where c is a certain positive constant.

Proof. Obviously (17) is equivalent to the same estimate for $x^{-11/2}A(x, h/k)$. To study

this, we divide (4) for $A(x, h/k)$ by $x^{11/2}$, and consider the right hand side choosing

$$N = \max(k^{-2}x, x^{1/2+\gamma}),$$

where γ is a positive constant to be chosen suitably. Then the error term is

$$\ll \min(k^2 x^r, x^{1/2-\gamma/2+\varepsilon}). \tag{18}$$

In the sum of length N, we estimate the initial terms with $n \leqslant k^{-1}x^{1/2}$ by absolute values, and apply Lemma 1 and the succeeding remark to the rest. The first mentioned terms contribute $\ll k^{1/4}x^{3/8}$.

Consider next those terms with $M \leqslant n \leqslant 2M$ for $k^{-1}x^{1/2} \leqslant M < N$. The parameters in Lemma 1 and in the remark for this sum are

$$F = k^{-1}(Mx)^{1/2}, \quad G = k^{1/2}M^{-3/4}x^{1/4}, \quad G' = G/M, \quad \theta = -\bar{h}/k.$$

Then we have $M \ll F$ if $M \leqslant k^{-2}x$, and otherwise $M \ll F^{1+d}$, where d depends on γ. Then the contribution to be estimated is

$$\ll k^{1/6}M^{-1/12}x^{5/12+\varepsilon} \ll k^{1/4}x^{3/8+\varepsilon}$$

if $M \ll k^{-2}x$, and otherwise this must perhaps be multiplied by a certain factor $F^{d'}$, where d' depends on γ. But in the latter case we have $k \gg x^{1/4-\gamma/2}$, and if we suppose that γ is small enough, then $k^{1/4}x^{3/8+\varepsilon}F^{d'}$ is dominated by the quantity in (18). Then (17) holds with $c = \gamma/3$.

For technical reasons, it is sometimes useful to provide sums or integrals with suitable smooth weights. In [4] we defined the weight function $\eta_J(x)$ in the interval $[a, b]$ as follows. Given a positive integer J and a positive number $U < (b-a)/2J$, we write for any integrable function h

$$U^{-J}\int_0^U \mathrm{d}u_1 \cdots \int_0^U \mathrm{d}u_J \int_{a+u}^{b-u} h(x)\,\mathrm{d}x = \int_a^b \eta_J(x)h(x)\,\mathrm{d}x, \tag{19}$$

where $u = u_1 + \cdots + u_J$. In addition, we define $\eta_0(x)$ to be the characteristic function of the interval $[a, b]$.

Exponential integrals can be approximately evaluated by the "saddle point method". The following saddle point lemma for smoothed exponential integrals is a simplified version of Theorem 2.2 from [4].

Lemma 3. Suppose that the function f satisfies the conditions of Lemma 1, and that $f''(x) > 0$ in the interval $[M, M']$. Suppose also that g is holomorphic and $g(z) \ll G$ in the domain D. Let $U > 0$, J a fixed non-negative integer, and $JU < (M' - M)/2$. Denote the characteristic function of the union of the intervals $(M, M + JU)$ and $(M' - JU, M')$ by $\delta(x)$, let α be a real number, x_0 the (possibly existing) zero of $f'(x) + \alpha$ in the interval (M, M'), and suppose that $U \gg \delta(x_0)F^{-1/2}M$. Write

$$E_J(x) = G(|f'(x) + \alpha| + F^{1/2}M^{-1})^{-J-1}.$$

Then

$$\int_M^{M'} \eta_J(x)g(x)e(f(x) + \alpha x)\,\mathrm{d}x = \xi_J(x_0)g(x_0)f''(x_0)^{-1/2}e(f(x_0) + \alpha x_0 + 1/8)$$

$$+O((1+\delta(x_0)F^{1/2})GMF^{-3/2})+O\Big(U^{-J}\sum_{j=0}^{J}(E_j(M+jU)+E_j(M'-jU))\Big),$$

where $\xi_J(x)$ *is bounded in the interval* (M, M'), $\xi_J(x)=1$ *for* $M+JU<x<M'-JU$, *and furthermore* $\xi_J'(x)$ *is continuous and* $\xi_J'(x)\ll U^{-1}$ *in the intervals* $(M+jU, M+(j+1)U)$ *and* $(M'-(j+1)U, M'-jU)$ *for* $j=0,1,\dots,J-1$. *If* x_0 *does not exist, then the terms and conditions involving* x_0 *are to be omitted.*

Remark. In Theorem 2.2 in [4], there is one more error term, but under the present assumptions it is absorbed by the others. The bound for $\xi_J'(x)$ given above is not included in Theorem 2.2, but it follows easily from the explicit expression for $\xi_J(x)$ in the theorem (which also shows that $\xi_1(x)$ is piecewise *linear*).

3. An estimate for a short exponential sum

As a preliminary for the proof of the theorem in the case (13), we show that the assertion (8) holds in a more precise form for sufficiently short sums.

Lemma 4. Suppose that α *is of the form (10)–(11), where* $K=x^{1/4}$, *and that (13) holds. Then there are positive constants a and b such that*

$$A(x_1, x; \alpha)\ll x^6 y^{-a} \tag{20}$$

for

$$x-x_1\ll|\eta|^{-1/2}x^{1/2+b}. \tag{21}$$

Proof. Suppose, for simplicity, that $\eta>0$. By partial summation, we have

$$A(x_1, x; \alpha)=A(x, h/k)e(x\eta)-A(x_1, h/k)e(x_1\eta)$$
$$-2\pi i\eta\int_{x_1}^{x}e(t\eta)A(t, h/k)\,\mathrm{d}t. \tag{22}$$

The first two terms are of the desired order by Lemma 2.

We replace $A(t, h/k)$ in the integral in (22) by its expression (3). The contribution of the error term is

$$\ll\eta^{1/2}k^{3/2}x^{23/4+b}\leqslant K^{1/2}x^{23/4+b}\leqslant x^{6-1/8+b},$$

which is admissible at least if $b<1/16$. The function $\cos(\dots)$ in (3) is written in terms of $e(\pm2\sqrt{nx}/k)$. The critical terms are those involving the negative sign, and the others can be treated similarly but more trivially. So the actual problem is to prove that

$$\eta k^{1/2}\sum_{n=1}^{\infty}\tilde{\tau}(n)e_k(-n\bar{h})n^{-3/4}I_n\ll x^{1/4}y^{-a}, \tag{23}$$

where

$$I_n=x^{-23/4}\int_{x_1}^{x}t^{23/4}e(\psi_n(t))\,\mathrm{d}t \tag{24}$$

and

$$\psi_n(t) = \eta t - 2\sqrt{nt}/k.$$

We integrated here a series term by term, which is justified by bounded convergence.

The order of I_n depends on the size of $|\psi_n'(t)|$ and $|\psi_n''(t)|$ in the interval of integration. Suppose that $|\psi_n^{(j)}(t)| \gg \lambda_j > 0$ for $j = 1$ or 2. Then it is well known that $I_n \ll \lambda_j^{-1/j}$. The derivative $\psi_n'(t)$ has a zero in $[x_1, x]$ if and only if $y_1 \leqslant n \leqslant y$, in which case we have to use $\lambda_2 \asymp \eta x^{-1}$. As to λ_1 for $n \notin [y_1, y]$, we have

$$\lambda_1 \gg \begin{cases} \eta y^{-1}(y_1 - n) & \text{for } n < y_1, \\ (kn^{1/2}x^{1/2})^{-1}(n - y) & \text{for } n > y. \end{cases} \tag{25}$$

Hence

$$I_n \ll \eta^{-1/2}x^{1/2} \quad \text{for } n \asymp y, \tag{26}$$

$$I_n \ll \eta^{-1}y(y_1 - n)^{-1} \quad \text{for } n < y_1, \tag{27}$$

$$I_n \ll kn^{1/2}x^{1/2}(n - y)^{-1} \quad \text{for } n > y. \tag{28}$$

Now the left hand side of (23) can be estimated by using (26) to (28). We obtain

$$\begin{aligned} &\ll (k^{1/2}y^{1/4} + \eta^{1/2}k^{1/2}x^{1/2}y^{-3/4}(y - y_1 + 1))y^{\varepsilon} \\ &\ll (k\eta^{1/2} + y^{-1/2} + k\eta x^{-1/2}(x - x_1))x^{1/4}y^{\varepsilon} \\ &\ll (k\eta^{1/2}x^{h} + y^{-1/2})x^{1/4}y^{\varepsilon}. \end{aligned} \tag{29}$$

Thus the assertion (23) holds if $k\eta^{1/2} \ll x^{-a_0}$ for some positive constant a_0 and $h < a_0/2$. Hence we may assume in the sequel that

$$k\eta^{1/2} \gg x^{-a_0}. \tag{30}$$

The constant a_0 will be chosen sufficiently small, in any case $a_0 < 1/16$. Then $y \gg k^{-2}x^{3/4} \gg x^{1/4}$, and thus the right hand side of (23) can be replaced by $x^{1/4-a}$ (on changing the meaning of a).

The argument leading to (29) shows that if those terms with

$$y^{1-\delta} \leqslant n \leqslant y^{1+\delta} \tag{31}$$

are excluded, then the estimate is improved by a factor $y^{-\delta/4}$. This saving is sufficient if $b < \delta/16$, so it remains to estimate the sum in (23) over the interval (31) in the case (30).

At this stage, we have to make a digression to the case $x - x_1 \ll x^{1/2}$. We claim there is a numerical constant a_1 such that

$$\tilde{A}(x_1, x; \xi) \ll x^{1/2-a_1}((x - x_1)x^{-1/2} + 1), \tag{32}$$

uniformly for all $x/2 \leqslant x_1 < x$ and all real ξ. The interesting case here is $x - x_1 \ll x^{1/2}$, for if this is settled, then the general result follows immediately.

We write a rational approximation to ξ as in (10) and (11), where $K = X^{1/4}$. Then either (12) or (13) holds for ξ. By (22) (with A replaced by $\tilde{A}$) and Lemma 2, we have

$$\tilde{A}(x_1, x; \xi) \ll (1 + \eta x^{1/2})x^{1/2-c}. \tag{33}$$

This implies (32) in the case (12).

Assuming now (13), we sharpen the argument leading to (29) on applying the trivial estimate $I_n \ll x^{1/2}$ instead of (26). In this way, we obtain an estimate for $A(x_1, x; \xi)$, and then

$$\tilde{A}(x_1, x; \xi) \ll k\eta^{1/2}x^{1/2+\varepsilon} + x^{1/2-c} \tag{34}$$

by partial summation.

There are two alternatives: either $k \leqslant Kx^{-c/2}$, or $Kx^{-c/2} < k \leqslant K$. In the former case,

$$k\eta^{1/2} \leqslant (k/K)^{1/2} \leqslant x^{-c/4},$$

and (32) follows from (34). In the latter case,

$$\eta x^{1/2} \leqslant (kK)^{-1}x^{1/2} \leqslant K^{-2}x^{1/2+c/2} = x^{c/2},$$

and (32) follows from (33).

We now return to (23). So far we have estimated terms on the left individually, but in the rest of the proof it is essential that some cancellation takes place in the sum over the interval $[y^{1-\delta}, y^{1+\delta}]$. The estimate (32) was proved for this purpose. It implies that if (30) holds and a_0 is sufficiently small, then there is an absolute constant a_2 such that

$$\sum_u^v \bar{\tau}(n)e_k(-n\bar{h})e(-2\sqrt{nt}/k) \ll (1 + (v-u)y^{-1/2})y^{1/2-a_2} \tag{35}$$

for all $t \in [x/2, x]$ and $y^{1-\delta} \leqslant u < v \leqslant y^{1+\delta}$. It suffices to prove this for $v - u \ll y^{1/2}$. Write the sum on the left as

$$\sum_u^v \bar{\tau}(n)e(n\xi)e(-n(\xi + \bar{h}/k) - 2\sqrt{nt}/k),$$

where $\xi = -\bar{h}/k - t^{1/2}u^{-1/2}k^{-1}$. By partial summation (32) and (30), this sum is

$$\ll (k^2\eta)^{-1}y^{1/2-a_1+3\delta/2} \ll x^{2a_0}y^{1/2-a_1+3\delta/2},$$

which is $\ll y^{1/2-a_1/2}$ if a_0 and δ are sufficiently small. Then we may choose $a_2 = a_1/2$.

Let now

$$Y \asymp \eta^{3/2}k^2x^{1/2+b},$$

be a number exceeding $2(y - y_1)$ (this is possible, for $y - y_1 \ll Y$). Consider first the sum over the interval $|n - y| \leqslant Y$ in (23). We invert the order of the summation and integration, apply (35), and estimate the integral trivially, to obtain

$$\ll (k\eta)^{1/2}y^{-1/4-a_2}x^{1/2+2b} \ll x^{1/4+2b-a_2/4},$$

which is $\ll x^{1/4-a}$ if a and b are chosen sufficiently small.

The sums over the intervals $[y^{1-\delta}, y - Y]$ and $[y + Y, y^{1+\delta}]$ can be estimated in the same way; consider the latter as an example. We subdivide the range of summation into segments $[y + \Delta, y + \Delta']$, where $Y \leqslant \Delta < \Delta' \leqslant 2\Delta \ll y^{1+\delta}$. The number of these is $\ll \log x$. We estimate the sum over one of the segments. By integration by parts, the

integral in (24) can be written as

$$\Big|_{x_1}^{x} t^{23/4} e(\psi_n(t))(\psi_n'(t))^{-1}$$

$$+ (1/2)k^{-1}n^{1/2} \int_{x_1}^{x} t^{17/4} e(\psi_n(t))(\psi_n'(t))^{-2}\, dt$$

$$- (23/4) \int_{x_1}^{x} t^{19/4} e(\psi_n(t))(\psi_n'(t))^{-1}\, dt. \tag{36}$$

The contribution of the integrated terms is estimated as above, and the result is of the order $O(x^{1/4-a})$ again. The integrands in the two integrals in (36) are at least by a factor x^{-2b} smaller in absolute value than the original integrand. If the integration by parts is repeated, then the integrands decrease at each step in the same way, until we end up with integrals which can be estimated trivially. The integrated terms can be dealt with like those in (36), and the proof of (23) is complete.

In retrospect, the crucial fact in the proof of Lemma 4 is seen to be the saving x^{-c} in (17) over the estimate $\ll x^{1/2}$.

4. Proof of the theorem

The case (12) can be settled by arguments similar to those in the proof of Lemma 4, or in [3], §4.1. It is to be shown that the last term on the right of (22) is $\ll x^6$. In fact, the estimate will be $\ll x^{23/4}k^{1/2} \ll x^{6-1/8}$. The point is that the exponential integrals occurring in the proof have no saddle point, because the bound 1/2 on the right of (12) is less than 1.

In the case (13), we have to prove the relation (14). To begin with, we replace $\tilde{A}(x_1, x; \alpha)$ by the smoothed sum

$$\tilde{A}_1(x_1, x; \alpha) = \sum_{x_1}^{x} \eta_1(n)\bar{\tau}(n)e(n\alpha), \tag{37}$$

where the weight function η_1 is constructed as in (19) on choosing $J = 1$ and $U = \eta^{-1/2}x^{1/2}y^b$ (the constant b is as in Lemma 4). The smoothing error is $\ll x^{1/2}y^{-a}$ by Lemma 4. Hence, as far as the proof of (14) is concerned, we may replace $\tilde{A}(x_1, x; \alpha)$ by the sum (37). It suffices to show that

$$\tilde{A}_1(x_1, x; \alpha) = (x/y)^{1/2}\tilde{A}(y_1, y; \beta) + O(x^{1/2}y^{-a}), \tag{38}$$

where the constant a is not necessarily the same as in Lemma 4.

We follow the argument in the proof of Theorem 5 (i) in [3], where an analogous formula with the error term $O(x^{1/2}\log x)$ was obtained for exponential sums involving $d(n)$. Without repeating the details of the proof, we indicate how the saving in the error term is achieved.

The sum (37) is first expanded by an identity (equation (1.9.2) in [4]), analogous to Voronoi's summation formula, as a series of exponential integrals. When these are

evaluated by Lemma 3, then the estimate for the contribution of the error terms turns out to be by a power of y smaller than that in [3]. The reason is that in [3] we had $U = \eta^{-1/2}x^{1/2}$, while the presence of the extra factor y^b in our parameter U improves the effect of the smoothing by a comparable saving factor. Also, Lemma 3 is more suitable for dealing with smoothed integrals than the saddle-point lemma applied in [3].

As to the main terms, Lemma 3 gives in the first place the sum

$$(x/y)^{1/2} \sum_{y_1 \leqslant n \leqslant y} w(n)\bar{\tau}(n)e(n\beta), \tag{39}$$

where β is as in (16), and $w(n) = \xi_1(n/(k\eta)^2)$ in the notation of Lemma 3; here $n/(k\eta)^2$ is the saddle point x_0 in the nth term. Since $\xi_1(u) = 1$ for $x_1 + U < u < x - U$, we have $w(n) = 1$ for $y_1 + k^2\eta^2 U < n < y - k^2\eta^2 U$. We make $w(n) = 1$ for all n, and estimate the error. Because $w(n)$ varies smoothly as a function of n, by Lemma 3, the error is by partial summation at most

$$\ll (x/y)^{1/2} \max_{u,v} |\tilde{A}(u, v; \beta)|, \tag{40}$$

where u and v lie either in the interval $[y_1, y_1 + k^2\eta^2 U]$ or in $[y - k^2\eta^2 U, y]$. The length of these intervals is $\asymp k^2\eta^{3/2}x^{1/2}y^b \ll y^{1/2+b}$. Hence, by (32), the maximum in (40) is $\ll y^{1/2-a}$ for some constant a if b is supposed to be smaller than the constant a_1 in (32). This means that the expression (39) can be written as $(x/y)^{1/2}\tilde{A}(y_1, y; \beta)$ with an error $\ll x^{1/2}y^{-a}$, and the assertion (38) follows.

References

[1] Apostol T M, Modular functions and Dirichlet series in number theory, in: *Graduate texts in mathematics* (New York, Heidelberg, Berlin: Springer Verlag) (1976)

[2] Deligne P, La conjecture de Weil, *Inst. Hautes Études Sci. Publ. Math.* **53** (1974) 273–307

[3] Jutila M, On exponential sums involving the divisor function. *J. Reine Angew. Math.* **355** (1985) 173–190

[4] Jutila M, Lectures on a method in the theory of exponential sums, in: *Lectures on mathematics and physics* (Bombay: Tata Institute of Fundamental Research) Vol. 80 (1987)

[5] Jutila M, Mean value estimates for exponential sums, *Journ. Arithm. Ulm* (1987) (to appear)

[6] Parson L A and Sheingorn M, Exponential sums connected with Ramanujan's function $\tau(n)$, *Mathematika* **29** (1982) 270–277

[7] Rankin R A, Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions II. The order of Fourier coefficients of integral modular forms, *Math. Proc. Cambridge Philos. Soc.* **35** (1939) 357–372

[8] Wilton J R, A note on Ramanujan's function $\tau(n)$, *Math. Proc. Cambridge Philos. Soc.* **25** (1929) 121–129

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 167–178.
© Printed in India.

Approximation of exponential sums by shorter ones

A A KARATSUBA
Steklov Mathematical Institute, Vavilova 42, 117966, Moscow GSP-1, USSR

Abstract. A new theorem on approximation of exponential sum by shorter one is proved.

Keyword. Exponential sums.

1. Introduction

This paper is dedicated to the centenary of S Ramanujan, whose works form a fundamental part of additive number theory—one of the largest areas in analytic number theory. A number of problems in the theory involve formulae of the kind

$$S = S_1 + R, \tag{1}$$

where

$$S = \sum_{a<x\leqslant b} \varphi(x)\exp[2\pi i f(x)],$$

$$S_1 = \sum_{\alpha<n\leqslant\beta} G(n)\exp[2\pi i F(n)],$$

$\varphi(x)$, $f(x)$, $G(n)$, $F(n)$ being some real functions, $b-a>\beta-\alpha>0$, and R—the "remainder" term. It seems that the first relations of type (1) with concrete functions φ, f, G, F were obtained by Vinogradov [5] and Hardy and Littlewood [1]. In a general form the theorem was proved by van der Corput [4] (c.f. also [3]). One of the most exact versions of (1) from the point of view of the estimate of R was proved by Vinogradov in [6]. In the conditions of Vinogradov's theorem algebraicity of the functions $\varphi(x)$ and $f'(x)$ was required. In [2] the present author proved (1) under weaker assumptions concerning $\varphi(x)$ and $f(x)$. A disadvantage of the theorem in [2] is the monotonicity condition, of a certain auxiliary function which, being controllable in every given case of applications seems nevertheless superfluous to a certain extent. Besides the estimate of the quantity R is rough. The aim of this paper is to present a new version of the proof of (1), which preserves the accuracy of Vinogradov's theorem and is close in the sense of the assumptions to those of van der Corput.

We use the following notations. For positive A the relations $B \ll A$, $A \gg B$ mean that $|B| \leqslant cA$, where $c>0$ is an absolute constant, $\|\alpha\| = \min(\{\alpha\}, 1-\{\alpha\})$, where $\{\alpha\}$ is the fractional part of α and for positive integer k, $f^{(k)}(x) = \mathrm{d}^k f(x)/\mathrm{d}x^k$.

2. Statement of the result

Theorem. *Let the real functions $f(x)$ and $\varphi(x)$ satisfy the following conditions on the segment $[a, b]$:*

b. There exist numbers $H, U, A, 0 < H, 1 \ll A \ll U, 0 < b - a \leqslant U$, *such that*

$$A^{-1} \ll f^{(2)}(x) \ll A^{-1}, \quad f^{(3)}(x) \ll A^{-1}U^{-1}, \quad f^{(4)}(x) \ll A^{-1}U^{-2},$$

$$\varphi(x) \ll H, \quad \varphi^{(1)}(x) \ll HU^{-1}, \quad \varphi^{(2)}(x) \ll HU^{-2}.$$

Then if we define the numbers x_n *from the equation*

$$f^{(1)}(x_n) = n,$$

we have

$$\sum_{a<x\leqslant b} \varphi(x)\exp[2\pi i f(x)] = \sum_{f^{(1)}(a)\leqslant n\leqslant f^{(1)}(b)} c(n)Z(n) + R, \tag{2}$$

where

$$R = O(HA(b-a)^{-1}) + O(HT_a) + O(HT_b) + O(H\ln(f^{(1)}(b) - f^{(1)}(a) + 2)), \tag{3}$$

$$T_\mu = \begin{cases} 0, & \text{if } f^{(1)}(\mu) \text{ is an integer} \\ \min\left(\dfrac{1}{\|f^{(1)}(\mu)\|}, \sqrt{A}\right), & \text{if } \|f^{(1)}(\mu)\| \neq 0, \end{cases}$$

$$c(n) = \begin{cases} 1, & \text{if } f^{(1)}(a) < n < f^{(1)}(b), \\ \frac{1}{2}, & \text{if } n = f^{(1)}(a) \text{ or } n = f^{(1)}(b), \end{cases}$$

$$Z(n) = \frac{1+i}{\sqrt{2}} \frac{\varphi(x_n)}{[f^{(2)}(x_n)]^{1/2}} \exp[2\pi i(f(x_n) - nx_n)]. \tag{4}$$

3. Lemmas

We prove two auxiliary statements.

Lemma 1. Let $f(x)$ *and* $\varphi(x)$ *be real functions, satisfying the following requirements on the segment* $[a, b]$:

(*a*) $f^{(2)}(x)$ *and* $\varphi^{(1)}(x)$—*are continuous*:
(*b*) $0 < f^{(2)}(x) \ll 1$;
(*c*) *there exist numbers* $0 < H$, $0 < b - a \leqslant U$, *such that*

$$\varphi(x) \ll H, \quad \varphi^{(1)}(x) \ll HU^{-1}.$$

Then for each $\Delta \in (0, 1)$ *the equality*

$$\sum_{a<x\leqslant b} \varphi(x)\exp[2\pi i f(x)] = \sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta} \int_a^b \varphi(x)\exp[2\pi i(f(x) - nx)]\,dx + O(H\ln(\beta - \alpha + 2)), \tag{5}$$

is valid, where $\alpha = f^{(1)}(a)$, $\beta = f^{(1)}(b)$ *and the factor in the sign* O *depends only on* Δ.

Proof. We assume that $b-a>10$, since in the contrary case the assertion of the lemma is trivial. Let $\varphi(x)=1$. Take a positive integer $m=[10U^2K]$, $K=1+|\alpha|+|\beta|$, and for $[a]+2\leqslant M\leqslant[b]-1$ consider the integral W_M,

$$W_M=\int_{-0\cdot5}^{0\cdot5}\frac{\sin(2m+1)\pi x}{\sin\pi x}\exp[2\pi i f(M+x)]\,\mathrm{d}x.$$

Since

$$\frac{\sin(2m+1)\pi x}{\sin\pi x}=\sum_{n=-m}^{m}\exp[2\pi i n x], \tag{6}$$

we have

$$\int_{-0\cdot5}^{0\cdot5}\frac{\sin(2m+1)\pi x}{\sin\pi x}\mathrm{d}x=1,$$

and consequently

$$W_M=\exp[2\pi i f(M)]+V_M,$$

where

$$V_M=\int_{-0\cdot5}^{0\cdot5}\frac{\sin(2m+1)\pi x}{\sin\pi x}\{\exp[2\pi i f(M+x)]-\exp[2\pi i f(M)]\}\,\mathrm{d}x.$$

To estimate $|V_M|$ from above we represent V_M as a sum of the following three integrals:

$$V_M=\int_{-1/m}^{1/m}+\int_{-1/2}^{-1/m}+\int_{1/m}^{1/2}.$$

We estimate the first integral on the right hand side, using the finite differences formula to the expression in paranthesis:

$$\int_{-1/m}^{1/m}\ll\int_{-1/m}^{1/m}\frac{|f^{(1)}(x)||x|\,\mathrm{d}x}{|x|}\ll\frac{K}{m}\ll\frac{1}{U}.$$

The second and the third integrals are treated in the same way. For example, the latter may be estimated by first integrating by parts as:

$$\int_{1/m}^{1/2}\frac{\sin(2m+1)\pi x}{\sin\pi x}(\exp[2\pi i f(M+x)]-\exp[2\pi i f(M)])\,\mathrm{d}x$$

$$=-\frac{\exp[2\pi i f(M+x)]-\exp[2\pi i f(M)]}{\sin\pi x}\cdot\frac{\cos(2m+1)\pi x}{(2m+1)\pi}\Bigg|_{1/m}^{1/2}$$

$$+\int_{1/m}^{1/2}\frac{\cos(2m+1)\pi x}{(2m+1)\pi}Y_x\,\mathrm{d}x,$$

where

$$Y_x=\frac{\exp[2\pi i f(M+x)]2\pi i f^{(1)}(M+x)}{\sin\pi x}$$

$$-\frac{(\exp[2\pi i f(M+x)]-\exp[2\pi i f(M)])\pi\cos\pi x}{\sin^2\pi x}.$$

The first summand is of the order $O(Km^{-1}) = O(U^{-1})$. Furthermore

$$Y_x \ll \frac{K}{|x|}, \quad \int_{1/m}^{1/2} \frac{\cos(2m+1)\pi x}{(2m+1)\pi} Y_x \, dx \ll \frac{K}{m} \ln m \ll \frac{1}{U}.$$

Thus

$$V_M \ll U^{-1}; \quad W_M = \exp[2\pi i f(M)] + O(U^{-1}).$$

If we sum up the latter expression with respect to M and use the definition of W_M and formula (6), we obtain:

$$\begin{aligned}
\sum_{a<x\leqslant b} \exp[2\pi i f(x)] &= \sum_{M=[a]+2}^{[b]-1} W_M + O(1) \\
&= \sum_{M=[a]+2}^{[b]-1} \int_{-0.5}^{0.5} \sum_{n=-m}^{m} \exp[2\pi i(f(M+x)-nx)]\,dx + O(1) \\
&= \sum_{n=-m}^{m} \sum_{M=[a]+2}^{[b]-1} \int_{M-0.5}^{M+0.5} \exp[2\pi i(f(x)-nx)]\,dx + O(1) \\
&= \sum_{n=-m}^{m} I_n + O(1), \qquad (7)
\end{aligned}$$

where

$$I_n = \int_{[a]+1.5}^{[b]-0.5} \exp[2\pi i(f(x)-nx)]\,dx.$$

Next we estimate the sum of the summands from (7) with $n < f^{(1)}(a) - \Delta$ and $n > f^{(1)}(b) + \Delta$, i.e. the sum Σ,

$$\Sigma = \sum_{-m\leqslant n<f^{(1)}(a)-\Delta} I_n + \sum_{f^{(1)}(b)+\Delta<n\leqslant m} I_n.$$

Integrating by parts we find:

$$\begin{aligned}
I_n &= \frac{\exp[2\pi i(f(x)-nx)]}{2\pi i(f^{(1)}(x)-n)}\bigg|_{a_1}^{b_1} + O\left(\int_{a_1}^{b_1} \frac{f^{(2)}(x)\,dx}{(f^{(1)}(x)-n)^2}\right) \\
&= \frac{\exp(\pi i n)}{2\pi i}\left(\frac{\exp[2\pi i f(b_1)]}{f^{(1)}(b_1)-n} - \frac{\exp[2\pi i f(a_1)]}{f^{(1)}(a_1)-n}\right) \\
&\quad + O\left(\frac{f^{(1)}(b_1)-f^{(1)}(a_1)}{(f^{(1)}(a_1)-n)(f^{(1)}(b_1)-n)}\right),
\end{aligned}$$

where $a_1 = [a] + 1{\cdot}5$, $b_1 = [b] - 0{\cdot}5$. Since the fractions

$$(f^{(1)}(b_1)-n)^{-1}, \quad (f^{(1)}(a_1)-n)^{-1}$$

for $-m \leqslant n < f^{(1)}(a) - \Delta$ and $f^{(1)}(b) + \Delta < n \leqslant m$ are monotonically increasing, $\exp(\pi i n) = (-1)^n$, we have

$$\sum \frac{(-1)^n}{f^{(1)}(b_1)-n} = O(1), \quad \sum \frac{(-1)^n}{f^{(1)}(a_1)-n} = O(1).$$

$$\frac{f^{(1)}(b_1)-f^{(1)}(a_1)}{(f^{(1)}(a_1)-n)(f^{(1)}(b_1)-n)}$$

increases monotonically and thus

$$\sum_{-m\leqslant n<f^{(1)}(a)-\Delta}\frac{f^{(1)}(b_1)-f^{(1)}(a_1)}{(f^{(1)}(a_1)-n)(f^{(1)}(b_1)-n)}\ll\frac{f^{(1)}(b_1)-f^{(1)}(a_1)}{\Delta(f^{(1)}(b_1)-f^{(1)}(a_1)+\Delta)}$$

$$+\int_{-m}^{f^{(1)}(a)-\Delta}\frac{f^{(1)}(b_1)-f^{(1)}(a_1)}{(f^{(1)}(a_1)-x)(f^{(1)}(b_1)-x)}\,\mathrm{d}x=O(\ln(\beta-\alpha+2)).$$

The sum of the fractions for $f^{(1)}(b)+\Delta<n\leqslant m$ is estimated analogously. Thus,

$$\sum=O(\ln(\beta-\alpha+2));$$

$$\sum_{a<x\leqslant b}\exp[2\pi i f(x)]=\sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta}I_n+O(\ln(\beta-\alpha+2)).$$

Let us substitute I_n for the integral over the interval (a, b):

$$I_n=\int_a^b\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x-I_{n,1}-I_{n,2},$$

where

$$I_{n,1}=\int_a^{a_1}\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x,\quad I_{n,2}=\int_{b_1}^b\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x.$$

Each segment $[\alpha-\Delta, f^{(1)}(a_1)+\Delta]$ and $[f^{(1)}(b_1)-\Delta, \beta+\Delta]$ can contain not more than $O(1)$ of integers n. Excluding those numbers for the remaining ones n we have the estimates

$$I_{n,1}=O(|f^{(1)}(a_1)-n|^{-1}+|\alpha-n|^{-1}),$$

$$I_{n,2}=O(|f^{(1)}(b_1)-n|^{-1}+|\beta-n|^{-1}).$$

Consequently

$$\sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta}(I_{n,1}+I_{n,2})=O(\ln(\beta-\alpha+2));$$

$$\sum_{a<x\leqslant b}\exp[2\pi i f(x)]=\sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta}\int_a^b\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x$$

$$+O(\ln(\beta-\alpha+2)).$$

Thus, our lemma is proved for $\varphi(x)=1$. Now let $\varphi(x)$ be an arbitrary function. If we apply the formula of summation by parts, we see that

$$\sum_{a<x\leqslant b}\varphi(x)\exp[2\pi i f(x)]=-\int_a^b\mathbb{C}(u)\varphi'(u)\,\mathrm{d}u+\mathbb{C}(b)\varphi(b),$$

where

$$\mathbb{C}(u)=\sum_{a<x\leqslant u}\exp[2\pi i f(x)].$$

We apply the already proved statement to $\mathbb{C}(u)$:

$$\mathbb{C}(u) = \sum_{\alpha-\Delta\leqslant n\leqslant\gamma+\Delta} \int_a^u \exp[2\pi i(f(x)-nx)]\,dx + O(\ln(\beta-\alpha+2)),$$

$$\gamma = f^{(1)}(u) \leqslant \beta;$$

as for $\gamma+\Delta < n \leqslant \beta+\Delta$

$$\int_a^u \exp[2\pi i(f(x)-nx)]\,dx = O\left(\frac{1}{n-\gamma}\right).$$

We have

$$\mathbb{C}(u) = \sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta} \int_a^u \exp[2\pi i(f(x)-nx)]\,dx + O(\ln(\beta-\alpha+2));$$

$$\sum_{a<x\leqslant b} \varphi(x)\exp[2\pi i f(x)] = -\sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta} \int_a^b \left(\int_a^u \exp[2\pi i(f(x)-nx)]\,dx\right)$$

$$\times\, \varphi^{(1)}(u)\,du + \sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta} \left(\int_a^b \exp[2\pi i(f(x)-nx)]\,dx\right)\varphi(b)$$

$$+ O(H\ln(\beta-\alpha+2)) = \sum_{\alpha-\Delta\leqslant n\leqslant\beta+\Delta} \int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,dx$$

$$+ O(H\ln(\beta-\alpha+2)),$$

which completes the proof of the lemma.

Lemma 2. Let $f(x)$ and $\varphi(x)$ be real functions satisfying the following conditions on the segment $[a,b]$:

(a) $f^{(4)}(x)$ and $\varphi^{(2)}(x)$ are continuous;

(b) there exist numbers H, U, A, $0<H$, $1 \ll A \ll U$, $0 < b-a \leqslant U$, such that

$$A^{-1} \ll f^{(2)}(x) \ll A^{-1}, \quad f^{(3)}(x) \ll A^{-1}U^{-1}, \quad f^{(4)}(x) \ll A^{-1}U^{-2},$$

$$\varphi \ll H, \quad \varphi^{(1)}(x) \ll HU^{-1}, \quad \varphi^{(2)}(x) \ll HU^{-2};$$

(c) for a certain c, $a \leqslant c \leqslant b$, $f'(c) = 0$.

Then the following formula is valid:

$$\int_a^b \varphi(x)\exp[2\pi i f(x)]\,dx = \frac{1+i}{\sqrt{2}}\frac{\varphi(c)\exp[2\pi i f(c)]}{[f^{(2)}(c)]^{1/2}} + O(HAU^{-1})$$

$$+ O\left(H_{\min}\left(\frac{1}{|f^{(1)}(a)|}, \sqrt{A}\right)\right) + O\left(H_{\min}\left(\frac{1}{|f^{(1)}(b)|}, \sqrt{A}\right)\right).$$

Proof. If we divide the interval of integration by the point c into two parts, we obtain:

$$\int_a^b \varphi(x)\exp[2\pi i f(x)]\,dx = \int_a^c + \int_c^b. \tag{8}$$

Compute the second integral. It is obvious that

$$\int_c^b \varphi(x)\exp[2\pi i f(x)]\,dx = \varphi(c)\int_c^b \exp[2\pi i f(x)]\,dx + \int_0^{b-c}(\varphi(x+c)-\varphi(c))\exp[2\pi i f(x+c)]\,dx.$$

Estimate the second integral of this formula. Integrating by parts, we get:

$$\int_0^{b-c}(\varphi(x+c)-\varphi(c))\exp[2\pi i f(x+c)]\,dx = \frac{\varphi(x+c)-\varphi(c)}{2\pi i f^{(1)}(x+c)}\exp[2\pi i f(x+c)]\Big|_0^{b-c} - \frac{1}{2\pi i}\int_0^{b-c}\frac{\varphi^{(1)}(x+c)f^{(1)}(x+c)-f^{(2)}(x+c)(\varphi(x+c)-\varphi(c))}{(f^{(1)}(x+c))^2}\exp[2\pi i f(x+c)]\,dx.$$

Since

$$\varphi(x+c)-\varphi(c) = \varphi^{(1)}(c)x + O(HU^{-1}x^2),$$

$$f^{(1)}(x+c) = f^{(2)}(c)x + O(A^{-1}U^{-1}x^2), \quad f^{(1)}(x+c) \gg xA^{-1} \text{ and}$$

$$f^{(2)}(x+c) = f^{(2)}(c) + O(A^{-1}U^{-1}x),$$

the first summand is of the order $O(HAU^{-1})$, and the absolute value of the integrand does not exceed

$$|\varphi^{(1)}(c) + O(HU^{-1}x))(f^{(2)}(c)x + O(A^{-1}U^{-1}x^2)) - (f^{(2)}(c) + O(A^{-1}U^{-1}x))(\varphi^{(1)}(c)x + O(HU^{-1}x^2))| \ll HA^{-1}U^{-2}x^2.$$

Thus the integral as a whole is $O(HAU^{-1})$. Now compare J and J_1 defined by

$$J = \int_0^{b-c}\exp[2\pi i f(x+c)]\,dx, \quad J_1 = \int_0^{b-c}\frac{f^{(1)}(x+c)\exp[2\pi i f(x+c)]\,dx}{[2f^{(2)}(c)(f(x+c)-f(c))]^{1/2}}.$$

Observing the difference $J - J_1$, let us integrate by parts. Then we find:

$$J - J_1 = \frac{1}{2\pi i}\left(\frac{1}{f^{(1)}(x+c)} - \frac{1}{[2f^{(2)}(c)(f(x+c)-f(c))]^{1/2}}\right)\exp[2\pi i f(x+c)]\Big|_0^{b-c} + O\left(\int_0^{b-c}\left|-\frac{f^{(2)}(x+c)}{(f^{(1)}(x+c))^2} + \frac{f^{(1)}(x+c)}{[8f^{(2)}(c)](f(x+c)-f(c))^{3/2}}\right|dx\right).$$

Using the relations

$$f(x+c)-f(c) = \tfrac{1}{2}f^{(2)}(c)x^2 + \tfrac{1}{6}f^{(3)}(c)x^3 + O(A^{-1}U^{-2}x^4),$$

$$f^{(1)}(x+c) = f^{(2)}(c)x + \tfrac{1}{2}f^{(3)}(c)x^2 + O(A^{-1}U^{-2}x^3) \text{ and}$$

$$f^{(2)}(x+c) = f^{(2)}(c) + f^{(3)}(c)x + O(A^{-1}U^{-2}x^2),$$

we easily find that the first summand is of the order $O(AU^{-1})$ while the integrand of the second one is $O(AU^{-2})$. Consequently,

$$J = J_1 + O(AU^{-1}).$$

We now compute J_1 by introducing the new variable of integration $f(x+c) - f(c) = u$. Denoting by λ the difference $f(b) - f(c)$, we obtain

$$J_1 = \frac{\exp[2\pi i f(c)]}{[2f^{(2)}(c)]^{1/2}} \int_0^{\lambda} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} = \frac{\exp[2\pi i f(c)]}{[2f^{(2)}(c)]^{1/2}} \int_0^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}}$$
$$- \frac{\exp[2\pi i f(c)]}{[2f^{(2)}(c)]^{1/2}} \int_{\lambda}^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}}.$$

We estimate the latter integral in two ways. First of all

$$\left| \int_{\lambda}^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} \right| \leqslant \int_{\lambda}^{\lambda+1} \frac{du}{\sqrt{u}} + \left| \int_{\lambda+1}^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} \right| \ll 1;$$

and besides, for $0 < \lambda$

$$\left| \int_{\lambda}^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} \right| \ll \frac{1}{\sqrt{\lambda}} = \frac{1}{[f(b) - f(c)]^{1/2}}.$$

Since

$$f(b) - f(c) = \tfrac{1}{2} f^{(2)}(\xi)(b-c)^2 \gg (b-c)^2 A^{-1},$$

$$|f^{(1)}(b)| = |f^{(1)}(b-c+c)| = f^{(2)}(\xi_1)(b-c) \ll (b-c)A^{-1},$$

we have

$$\frac{1}{[f(b) - f(c)]^{1/2}} \ll \frac{\sqrt{A}}{b-c} \ll \frac{1}{|f^{(1)}(b)|\sqrt{A}}.$$

Thus we obtain that

$$J_1 = \frac{\exp[2\pi i f(c)]}{[2f^{(2)}(c)]^{1/2}} \int_0^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} + O\left(\min\left(\frac{1}{|f^{(1)}(b)|}, \sqrt{A}\right)\right);$$

$$\int_c^b = \frac{\varphi(c)\exp[2\pi i f(c)]}{[2f^{(2)}(c)]^{1/2}} \int_0^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} + O(HAU^{-1})$$
$$+ O\left(H_{\min}\left(\frac{1}{|f^{(1)}(b)|}, \sqrt{A}\right)\right).$$

The first integral in (8) is computed in an analogous manner:

$$\int_a^c = \frac{\varphi(c)\exp[2\pi i f(c)]}{[2f^{(2)}(c)]^{1/2}} \int_0^{\infty} \frac{\exp(2\pi i u)\,du}{\sqrt{u}} + O(HAU^{-1})$$
$$+ O\left(H_{\min}\left(\frac{1}{|f^{(1)}(a)|}, \sqrt{A}\right)\right).$$

Since

$$\int_0^\infty \frac{\cos 2\pi u\,\mathrm{d}u}{\sqrt{u}} = \int_0^\infty \frac{\sin 2\pi u\,\mathrm{d}u}{\sqrt{u}} = \frac{1}{2},$$

the proved relations imply the statement of the lemma.

Remark. If we estimate the right hand side of the formula of the lemma trivially, we obtain

$$\left| \int_a^b \varphi(x) \exp\left[2\pi i f(x)\right] \mathrm{d}x \right| \ll H\sqrt{A}.$$

The above estimate is valid also under weaker assumptions concerning the functions $f(x)$ and $\varphi(x)$, namely, if $f^{(2)}(x)$ and $\varphi^{(1)}(x)$ are continuous on $[a, b]$ and, besides,

$$A^{-1} \ll f^{(2)}(x) \ll A^{-1}, \quad \varphi(x) \ll H, \quad \varphi^{(1)}(x) \ll HU^{-1}, \quad a \leqslant x \leqslant b.$$

Let us prove it. We can assume, with no loss of generality, that $b - a \geqslant 4\sqrt{A}$. If the root, say c, of the equation $f^{(1)}(x) = 0$ belongs to the segment $[a, b]$, then we use the equality

$$\int_a^b = \int_a^{c-\sqrt{A}} + \int_{c-\sqrt{A}}^{c+\sqrt{A}} + \int_{c+\sqrt{A}}^b.$$

and estimate each of the three appearing integrals. The integral in the middle is estimated trivially:

$$\int_{c-\sqrt{A}}^{c+\sqrt{A}} \ll H\sqrt{A}.$$

The integrals on the extremes are estimated in the same way. E.g., consider the first one. We can assume that $a < c - \sqrt{A}$. Integrating by parts we find:

$$\int_a^{c-\sqrt{A}} \varphi(x) \exp\left[2\pi i f(x)\right] \mathrm{d}x = \frac{1}{2\pi i} \frac{\varphi(x)}{f^{(1)}(x)} \exp\left[2\pi i f(x)\right] \Bigg|_a^{c-\sqrt{A}}$$

$$- \frac{1}{2\pi i} \int_a^{c-\sqrt{A}} \frac{\varphi^{(1)}(x) f^{(1)}(x) - \varphi(x) f^{(2)}(x)}{(f^{(1)}(x))^2} \exp\left[2\pi i f(x)\right] \mathrm{d}x.$$

Since $f^{(1)}(x)$ is monotonically increasing,

$$f^{(1)}(c) = 0, \quad a \leqslant c \leqslant b, \quad |f^{(1)}(a)| \geqslant |f^{(1)}(c - \sqrt{A})| \gg A^{-0.5}$$

and the first summand of the latter formula are of the order $H\sqrt{A}$. The second summand, i.e. the integral, is estimated trivially, using that

$$f^{(1)}(x) = f^{(1)}(c + x - c) = f^{(2)}(\xi)(x - c),$$

we find

$$\int_a^{c-\sqrt{A}} \ll \int_a^{c-\sqrt{A}} \frac{HU^{-1}AU + HA^{-1}}{A^{-2}(x-c)^2} \mathrm{d}x \ll H\sqrt{A}.$$

On the other hand, if c does not belong to $[a, b]$, we represent the integral in the form

$$\int_a^b = \int_a^{a+\sqrt{A}} + \int_{a+\sqrt{A}}^{b-\sqrt{A}} + \int_{b-\sqrt{A}}^b .$$

The integrals on the extremes are trivially estimated by the quantity $\ll H\sqrt{A}$. The integral in the middle is estimated by means of partial integration:

$$\int_{a+\sqrt{A}}^{b-\sqrt{A}} \varphi(x)\exp[2\pi i f(x)]\,\mathrm{d}x = \frac{\varphi(x)}{2\pi i f^{(1)}(x)}\exp[2\pi i f(x)]\Big|_{a+\sqrt{A}}^{b-\sqrt{A}}$$

$$-\frac{1}{2\pi i}\int_{a+\sqrt{A}}^{b-\sqrt{A}} \frac{\varphi^{(1)}(x)f^{(1)}(x) - \varphi(x)f^{(2)}(x)}{(f^{(1)}(x))^2}\exp[2\pi i f(x)]\,\mathrm{d}x.$$

If $f^{(1)}(x) > 0$ for $a \leqslant x \leqslant b$, then

$$f^{(1)}(b-\sqrt{A}) > f^{(1)}(a+\sqrt{A}) = f^{(1)}(a) + f^{(2)}(\xi)\sqrt{A} \gg A^{-0.5},$$

$$f^{(1)}(x) = f^{(1)}(a+x-a) \gg A^{-1}(x-a).$$

Thus the first summand is of the order $O(H\sqrt{A})$.

The second summand, i.e. the integral, is estimated trivially:

$$\int_{a+\sqrt{A}}^{b-\sqrt{A}} \ll \int_{a+\sqrt{A}}^{b-\sqrt{A}} \left(\frac{HU^{-1}A}{x-a} + \frac{HA}{(x-a)^2}\right)\mathrm{d}x$$

$$\ll HU^{-1}A\ln(b-a) + H\sqrt{A} \ll H\sqrt{A}.$$

On the other hand, if $f^{(1)}(x) < 0$, then the estimation runs in an analogous way. Thus, the statement of the remark is proved.

4. Proof of the theorem

At first, let $\| f^{(1)}(a)\| \neq 0$, $\| f^{(1)}(b)\| \neq 0$. Take $\Delta = \frac{1}{2}$ in lemma 1; then we find:

$$\sum_{a\leqslant x\leqslant b} \varphi(x)\exp[2\pi i f(x)]$$

$$= \sum_{f^{(1)}(a)-\frac{1}{2}\leqslant n\leqslant f^{(1)}(b)+\frac{1}{2}} \int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x$$

$$+ O(H\ln(f^{(1)}(b) - f^{(1)}(a) + 2)). \tag{9}$$

Obviously,

$$f^{(1)}(a) < [f^{(1)}(a)] + 1, \quad [f^{(1)}(b)] < f^{(1)}(b).$$

If $[f^{(1)}(a)] + 1 \leqslant n \leqslant [f^{(1)}(b)]$ we apply lemma 2 to the integrals

$$\int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x,$$

taking $f(x)$ as $f(x)-nx$ and c as x_n. Then we have:

$$\int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x = \frac{1+i}{\sqrt{2}}\frac{\varphi(x_n)\exp[2\pi i(f(x_n)-nx_n)]}{[f^{(2)}(x_n)]^{1/2}}$$

$$+ O(HAU^{-1}) + O\left(H_{\min}\left(\frac{1}{|f^{(1)}(a)-n|}, \sqrt{A}\right)\right)$$

$$+ O\left(H_{\min}\left(\frac{1}{|f^{(1)}(b)-n|}, \sqrt{A}\right)\right).$$

Summing the above relation with respect to n, $[f^{(1)}(a)] < n \leqslant [f^{(1)}(b)]$ we get:

$$\sum_{[f^{(1)}(a)]<n\leqslant[f^{(1)}(b)]} \int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x$$

$$= \frac{1+i}{\sqrt{2}} \sum_{f^{(1)}(a)\leqslant n\leqslant f^{(1)}(b)} \frac{\varphi(x_n)\exp[2\pi i(f(x_n)-nx_n)]}{[f^{(2)}(x_n)]^{1/2}}$$

$$+ O\left(H_{\min}\left(\frac{1}{\|f^{(1)}(a)\|}, \sqrt{A}\right)\right) + O\left(H_{\min}\left(\frac{1}{\|f^{(1)}(b)\|}, \sqrt{A}\right)\right)$$

$$+ O(H\ln(f^{(1)}(b)-f^{(1)}(a)+2)).$$

The right hand side of (9) may contain additional summands of the form

$$\int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x,$$

where $n=[f^{(1)}(a)]$ or $n=[f^{(1)}(b)]+1$. In those cases $(\mathrm{d}/\mathrm{d}x)(f(x)-nx)\neq 0$ for $a\leqslant x\leqslant b$. Thus integrating by parts and estimating the right hand side trivially, after this we obtain:

$$\int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x = \frac{\varphi(x)}{2\pi i(f^{(1)}(x)-n)}\exp[2\pi i(f(x)-nx)]\Big|_a^b$$

$$-\frac{1}{2\pi i}\int_a^b \frac{\varphi^{(1)}(x)(f^{(1)}(x)-n)-\varphi(x)f^{(2)}(x)}{(f^{(1)}(x)-n)^2}\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x$$

$$\ll \frac{H}{\|f^{(1)}(\mu)\|},$$

where $\mu=a$, if $n=[f^{(1)}(a)]$ and $\mu=b$, if $n=[f^{(1)}(b)]+1$. According to the remark following lemma 2 we have also the estimate

$$\int_a^b \varphi(x)\exp[2\pi i(f(x)-nx)]\,\mathrm{d}x \ll H\sqrt{A}.$$

Thus, the statement of the theorem is proved in the case $\|f^{(1)}(a)\|\neq 0$, $\|f^{(1)}(b)\|\neq 0$.

Now, let $\| f^{(1)}(a) \| = 0$, i.e. $f^{(1)}(a)$ is an integer, $\| f^{(1)}(b) \| \neq 0$. Again according to lemma 1, the relation is valid. Extracting the summand corresponding to $n = f^{(1)}(a)$ from the right hand side we apply the above observations to the remaining sum. We get:

$$\sum_{a<x\leqslant b} \varphi(x) \exp[2\pi i f(x)] = \int_a^b \varphi(x) \exp[2\pi i(f(x) - f^{(1)}(a)x)]\,dx$$

$$+ \frac{1+i}{\sqrt{2}} \sum_{f^{(1)}(a)<n\leqslant f^{(1)}(b)} \frac{\varphi(x_n) \exp[2\pi i(f(x_n) - nx_n)]}{[f^{(2)}(x_n)]^{1/2}}$$

$$+ O\left(H_{\min}\left(\frac{1}{\| f^{(1)}(b) \|}, \sqrt{A} \right) \right) + O(H \ln(f^{(1)}(b) - f^{(1)}(a) + 2)).$$

Here, the first integral was computed in lemma 2 (with $c = a$) and it equals

$$\frac{1+i}{2\sqrt{2}} \frac{\varphi(a) \exp[2\pi i(f(a) - f^{(1)}(a)a)}{[f^{(2)}(a)]^{1/2}} + O(HA(b-a)^{-1}).$$

This implies that the assertion of the theorem is valid for $\| f^{(1)}(a) \| = 0$, $\| f^{(1)}(b) \| \neq 0$ as well. The assertion of the theorem in the other two remaining cases, namely, for $\| f^{(1)}(a) \| \neq 0$, $\| f^{(1)}(b) \| = 0$ and for $\| f^{(1)}(a) \| = \| f^{(1)}(b) \| = 0$ is proved analogously. The theorem is completely proved.

References

[1] Hardy G H and Littlewood J E, The zeros of Riemann's zeta-function on the critical line, *Math. Z.* **10** (1921) 283–317

[2] Karatsuba A A, *Fundamentals of analytic theory of numbers* (Moscow: Nauka) II edn (1983)

[3] Titchmarsh E K, *Theory of Riemann's zeta-functions* (Oxford: University Press) (1951)

[4] Van der Corput J G, Verschärfung der abschätzung beim teilerproblem, *Math. Ann.* **87** (1922) 39–65

[5] Vinogradov I M, *On the average value of the number of classes of purely root form of the negative determinant, Communications of Kharkhov Mathematics Society*, vol. 16 (1917) pp. 10–38

[6] Vinogradov I M, *Special versions of the methods of trigonometric sums* (Moscow: Nauka) (1978)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 179–188.
© Printed in India.

On endomorphisms of degree two

MAX KOECHER
Mathematisches Institut der Westfälischen-Wilhelms-Universität Münster,
Einsteinstraße 62, 4400 Münster, FRG

Abstract. Let R be a commutative ring, $\Delta \in R$ and let $R\{\Delta\}$ be the set of conjugacy classes of R-module endomorphisms f satisfying $f \circ f = \Delta \cdot id$. Using a certain subspace of the tensor product of two endomorphisms a commutative and associative product on $R\{\Delta\}$ can be defined. For $R = \mathbb{Z}$ a generalization of the composition of quadratic forms arises as a special case.

Keywords. Composition of quadratic forms; commutative rings; tensor products; conjugacy class of endomorphism.

1. Introduction

Let R be a commutative ring with unit element $1 = 1_R$ and let Δ be an element of R. A pair (A, f) is called a Δ-*pair*, if A is an R-module and $f: A \to A$ is a linear mapping satisfying $f \circ f = \Delta \cdot i$, where $i: A \to A$ denotes the identity mapping.

Given two Δ-pairs (A, f) and (B, g) there is a natural way to construct a new Δ-pair $(A * B, f * g)$. This construction is compatible with homomorphisms of Δ-pairs and hence induces a commutative and associative composition on the set $R\{\Delta\}$ of isomorphism classes of Δ-pairs.

In the case of free $\mathbb{Z}$-modules of rank 2 the composition is isomorphic to the product of the ideal classes in the ring $\mathbb{Z}[\sqrt{\Delta}]$ provided that Δ is not a square in $\mathbb{Z}$. Hence we obtain a new description of the composition of binary quadratic forms over $\mathbb{Z}$ in the sense of C F Gauss.

2. Δ-pairs

Suppose that (A, f) and (B, g) are Δ-pairs. The elements of A resp. B are written as a, a_1, a_2 etc. resp. b, b_1, b_2 etc. A linear mapping $\varphi: A \to B$ is called a *homomorphism of the* Δ-*pairs*, if

$$\varphi \circ f = g \circ \varphi \tag{1}$$

holds. We also write $\varphi: (A, f) \to (B, g)$.

Now consider the tensor product $A \otimes B$ over R and the submodule

$$A * B := (f \otimes i + i \otimes g)(A \otimes B) \tag{2}$$

of $A \otimes B$. Clearly, $A * B$ is spanned by the elements

$$a * b := f(a) \otimes b + a \otimes g(b), \quad \text{where} \quad a \in A \quad \text{and} \quad b \in B. \tag{3}$$

Using

$$(f \otimes i)(a * b) = \Delta a \otimes b + f(a) \otimes g(b) = (i \otimes g)(a * b) \tag{4}$$

a linear mapping $f * g: A * B \to A * B$ is defined by

$$f * g := f \otimes i|_{A*B} = i \otimes g|_{A*B}. \tag{5}$$

PROPOSITION A.

Suppose that (A, f) and (B, g) are Δ-pairs. Then $(A, f) * (B, g) := (A * B, f * g)$ becomes a Δ-pair, too.

Proof. Clearly,

$$(f * g) \circ (f * g) = (f \otimes i) \circ (f \otimes i)|_{A*B} = (f \circ f) \otimes i|_{A*B} = \Delta \cdot i \otimes i|_{A*B}$$

in view of (5). □

Applying $i \otimes g$ to (4) yields

$$(f \otimes g)(x) = \Delta \cdot x, \quad \text{whenever} \quad x \in A * B. \tag{6}$$

PROPOSITION B.

Suppose that $\varphi: (A, f) \to (\bar{A}, \bar{f})$ and $\psi: (B, g) \to (\bar{B}, \bar{g})$ are homomorphisms of the Δ-pairs. Then

$$\chi: A * B \to \bar{A} * \bar{B}, \quad \chi := \varphi \otimes \psi|_{A*B},$$

becomes a homomorphism of the Δ-pairs.

Proof. First of all, write $\bar{a} := \varphi(a)$ resp. $\bar{b} = \psi(b)$, and obtain

$$\overline{f(a)} = \bar{f}(\bar{a}) \quad \text{resp.} \quad \overline{g(b)} = \bar{g}(\bar{b})$$

from (1). Hence

$$\chi(a * b) = \overline{f(a)} \otimes \bar{b} + \bar{a} \otimes \overline{g(b)} = \bar{f}(\bar{a}) \otimes \bar{b} + \bar{a} \otimes \bar{g}(\bar{b}) \in \bar{A} * \bar{B} \tag{*}$$

holds according to (3). In order to prove $\chi \circ (f * g) = (\bar{f} * \bar{g}) \circ \chi$ it suffices to consider elements of the form (3). Hence one gets

$$\chi \circ (f * g)(a * b) = \chi(f(a) * b) = \bar{f}(\overline{f(a)}) \otimes \bar{b} + \overline{f(a)} \otimes \bar{g}(\bar{b})$$

$$= (\bar{f} \otimes i)(\bar{f}(\bar{a}) \otimes \bar{b} + \bar{a} \otimes \bar{g}(\bar{b})) = (\bar{f} l * \bar{g}) \circ \chi(a * b)$$

using (5) and (*). □

PROPOSITION C.

Suppose that (A, f) and (B, g) are Δ-pairs. Then the restriction φ of the mapping $A \otimes B \to B \otimes A$ given by $a \otimes b \mapsto b \otimes a$ to $A * B$ becomes an isomorphism of $A * B$ onto $B * A$ and satisfies $\varphi(a * b) = b * a$.

Proof. Clearly,

$$\varphi(a * b) = g(b) \otimes a + b \otimes f(a) = b * a$$

holds according to (3). Hence

$$\varphi \circ (f * g)(a * b) = \varphi(\Delta a \otimes b + f(a) \otimes g(b)) = \Delta \cdot b \otimes a + g(b) \otimes f(a),$$

$$(g * f) \circ \varphi(a * b) = (g * f)(b * a) = \Delta b \otimes a + g(b) \otimes f(a)$$

follow from (4) and (5). □

In order to prove the associative law start with three Δ-pairs (A, f), (B, g), (C, h) and compute

$$\begin{aligned}(a * b) * c &= [(f * g)(a * b)] \otimes c + (a * b) \otimes h(c) \\ &= [\Delta \cdot a \otimes b + f(a) \otimes g(b)] \otimes c + [f(a) \otimes b + a \otimes g(b)] \otimes h(c) \\ &= \Delta \cdot [a \otimes b] \otimes c + [f(a) \otimes g(b)] \otimes c \\ &\quad + [f(a) \otimes b] \otimes h(c) + [a \otimes g(b)] \otimes h(c)\end{aligned}$$

according to (3), (4) and (5). With the aid of similar arguments one obtains

$$\begin{aligned}a * (b * c) &= \Delta \cdot a \otimes [b \otimes c] + f(a) \otimes [g(b) \otimes c] \\ &\quad + f(a) \otimes [b \otimes h(c)] + a \otimes [g(b) \otimes h(c)].\end{aligned}$$

Furthermore one calculates

$$\begin{aligned}([f * g] * h)([a * b] * c) &= \Delta \cdot (a * b) \otimes c + [(f * g)(a * b)] \otimes h(c) \\ &= \Delta \cdot [f(a) \otimes b] \otimes c + \Delta \cdot [a \otimes g(b)] \otimes c \\ &\quad + \Delta \cdot [a \otimes b] \otimes h(c) + [f(a) \otimes g(b)] \otimes h(c)\end{aligned}$$

and respectively.

$$\begin{aligned}&(f * [g * h])(a * [b * c]) \\ &= \Delta \cdot a \otimes [b * c] + f(a) \otimes [(g * h)(b * c)] \\ &= \Delta \cdot a \otimes [g(b) \otimes c] + \Delta \cdot a \otimes [b \otimes h(c)] + \Delta \cdot f(a) \otimes [b \otimes c] \\ &\quad + f(a) \otimes [g(b) \otimes h(c)].\end{aligned}$$

$$(A \otimes B) \otimes C \to A \otimes (B \otimes C),\ (a \otimes b) \otimes c \mapsto a \otimes (b \otimes c),$$

to $(A*B)*C$. Hence one has

$$\chi(a*(b*c)) = (a*b)*c$$

and

$$\chi^{\circ}([f*g]*h) = (f*[g*h])^{\circ}\chi$$

holds. A summary yields

PROPOSITION D.

Suppose that $(A, f), (B, g)$ and (C, h) are Δ-pairs. Then the mapping $\chi: (A*B)*C \to A*(B*C)$ becomes an isomorphism of the Δ-pairs.

Now let $R\{\Delta\}$ denote the set of isomorphism classes of Δ-pairs over the ring R. The isomorphism class of a Δ-pair (A, f) is denoted by

$$\mathfrak{a} = \not< A, f \not>. \tag{7}$$

According to Proposition A and B a product is defined in $R\{\Delta\}$ via

$$\mathfrak{a}*\mathfrak{b} := \not< A*B, f*g \not>, \quad \text{whenever} \quad \mathfrak{a} = \not< A, f \not>, \quad \mathfrak{b} = \not< B, g \not>. \tag{8}$$

The propositions C and D lead to the

Lemma. The set $R\{\Delta\}$ of isomorphism classes of Δ-pairs forms a commutative semi-group.

3. Free modules

Let R^m denote the free R-module of column vectors with m entries. As an example consider a Δ-pair (A, f), where A is a free R-module of rank $m \geqslant 1$. Let $\mathscr{A} = (a_1, \ldots, a_m)$ be a basis of A and put

$$h(a) := \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}, \tag{9}$$

whenever $a = \alpha_1 a_1 + \cdots + \alpha_m a_m$ and $\alpha_1, \ldots, \alpha_m \in R$. Hence $h = h_{\mathscr{A}}: A \to R^m$ becomes a bijective linear mapping and there exists a matrix $F \in \mathrm{Mat}(m; R)$ such that

$$h \circ f = F \circ h, \quad F^2 = \Delta \cdot I, \tag{10}$$

holds. Clearly, $h: (A, f) \to (R^m, F)$ becomes an isomorphism of the Δ-pairs.

Suppose further that (B, g) is a Δ-pair, where B is a free R-module of rank n and that $\mathscr{B} = (b_1, \ldots, b_n)$ is a basis of B. How can the product $(A*B, f*g)$ be described?

Consider the diagram

$$\begin{array}{ccc} (A,f)\times(B,g) & \to (A*B, f*g), & (a,b)\mapsto a*b, \\ {\scriptstyle h_{\mathcal{A}}}\downarrow & \downarrow{\scriptstyle h_{\mathcal{B}}} & \\ (R^m,F)\times(R^n,G)\to(R^m*R^n, F*G). & & \end{array} \tag{11}$$

In order to describe the module $A*B$, or better the module R^m*R^n, consider the isomorphism $\Phi\colon R^m\otimes R^n\to \mathrm{Mat}(m,n;R)$ induced by $\Phi(a\otimes b):=ab^t$, where b^t stands for the transpose of b.

Hence the subspace

$$R^m*R^n=(F\otimes I+I\otimes G)(R^m\otimes R^n)$$

of $R^m\otimes R^n$ is spanned by

$$z:=Fx\otimes y+x\otimes Gy, \quad \text{where} \quad x\in R^m, \quad y\in R^n, \tag{12}$$

and the map $F*G$ is given by

$$(F*G)(z):=\Delta\cdot x\otimes y+Fx\otimes Gy. \tag{12'}$$

Now the image $\Phi(R^m*R^n)$ is spanned by the matrices

$$(Fx)y^t+x\cdot(Gy)^t=F\cdot xy^t+xy^t\cdot G^t.$$

Hence

$$\Phi(R^m*R^n)=\{FM+MG^t;\, M\in\mathrm{Mat}(m,n;R)\} \tag{13}$$

holds. In addition, the map $F*G$ is given via

$$FM+MG^t\mapsto F(FM+MG^t)=\Delta\cdot M+FMG^t \tag{13'}$$

in view of (4). A summary yields the

Lemma. Suppose that (A,f) and (B,g) are Δ-pairs, where A resp. B are free R-modules of rank m resp. n. Then the Δ-pair $(A*B, f*g)$ is isomorphic to the Δ-pair (C,h), where

$$C:=C_{F,G}:=\{FM+MG^t;\, M\in\mathrm{Mat}(m,n;R)\} \tag{14}$$

and where

$$h(X):=FX=XG^t, \quad \textit{whenever} \quad X\in C. \tag{14'}$$

Consider the Δ-pair (R^2,e), where $e\colon R^2\to R^2$ is given by

$$e(a):=Ea, \quad E:=\begin{pmatrix}0 & \Delta\\ 1 & 0\end{pmatrix}. \tag{15}$$

COROLLARY.

Suppose that (A,f) is a Δ-pair, where A is a free R-module. Then the Δ-pair $(A,f)*(R^2,e)$ is isomorphic to (A,f).

Proof. Without restriction suppose $A = R^m$ and $f(a) = Fa$, where $F \in \mathrm{Mat}(m; R)$ and $F^2 = \Delta \cdot I$. Hence according to (14), one has

$$C = \{FM + ME'; M \in \mathrm{Mat}(m, 2; R)\}$$
$$= \{(Fa + \Delta b, Fb + a); a, b \in R^m\}$$
$$= \{(Fc, c); c \in R^m\} \cong R^m$$

and the mapping $h: C \to C$ corresponds to the endomorphism $c \mapsto Fc$ of R^m. □

The isomorphisms of (R^m, F) onto $(R^m, \tilde{F})$ clearly are given by matrices $W \in GL(m; R)$ such that $WF = \tilde{F}W$. Hence the isomorphism class $\not\in R^m, F\not\ni$ in $R\{\Delta\}$ coincides with the conjugacy class of the matrix F with respect to the group $GL(m; R)$.

PROPOSITION.

Suppose that R is a field of characteristic $\neq 2$ and suppose that Δ is a square in R. Then $R\{\Delta\}$ is isomorphic to the multiplicative semi-group $\mathbb{N} \times \mathbb{N}$.

Proof. A set of representatives of conjugacy classes of matrices $F \in \mathrm{Mat}(m; R)$ satisfying $F^2 = \Delta \cdot 1$ is given by

$$F_{p,q} := \sqrt{\Delta} \begin{pmatrix} I^{(p)} & 0 \\ 0 & -I^{(q)} \end{pmatrix}, \tag{16}$$

where $p + q = m$, and it is parametrized by $(p, q) \in \mathbb{N} \times \mathbb{N}$. Hence

$$F_{p,q}M + MF_{r,s} = 2\sqrt{\Delta} \begin{pmatrix} A & 0 \\ 0 & -D \end{pmatrix}, \tag{*}$$

where

$$M = \begin{pmatrix} A^{(p,r)} & B^{(p,s)} \\ C^{(q,r)} & D^{(q,s)} \end{pmatrix}.$$

Clearly, the dimension of $(R^m, F_{p,q}) * (R^n, F_{r,s})$ becomes $pr + qs$ and multiplication of (*) from the left hand side by $F_{p,q}$ produces the identity on $A \in \mathrm{Mat}(p, r; R)$ and minus the identity on $B \in \mathrm{Mat}(q, s; R)$. □

4. An obvious generalization

In order to generalize Δ-pairs consider a monic polynomial $\pi \in R[X]$ of degree $r \geqslant 1$

$$\pi(X) = \pi_0 + \pi_1 X + \cdots + \pi_{r-1} X^{r-1} + X^r, \tag{17}$$

where $\pi_0, \ldots, \pi_{r-1} \in R$. A pair (A, f) is now called a *π-pair*, if A is an R-module and if $f: A \to A$ is a linear mapping satisfying

$$\pi(f) = \pi_0 i + \pi_1 f + \cdots + \pi_{r-1} f^{r-1} + f^r = 0. \tag{18}$$

Suppose that (A, f) and (B, g) are π-pairs. Define a linear mapping $F_{f,g}: A \otimes B \to A \otimes B$ via

$$F_{f,g} := \sum_{k=0}^{r-1} \pi_{k+1} \sum_{\nu+\mu=k} f^{\nu} \otimes g^{\mu}, \quad \pi_r = 1. \tag{19}$$

In particular, one has

r	$F_{f,g}$
1	$i \otimes i$
2	$f \otimes i + i \otimes g + \pi_1 \cdot i \otimes i$
3	$f^2 \otimes i + f \otimes g + i \otimes g^2 + \pi_2 \cdot (f \otimes i + i \otimes g) + \pi_1 \cdot i \otimes i.$

A verification using (18) leads to

$$(f \otimes i) \circ F_{f,g} = F_{f,g} \circ (f \otimes i) = F_{f,g} \circ (i \otimes g) = (i \otimes g) \circ F_{f,g}. \tag{20}$$

Now writing

$$A * B := F_{f,g}(A \otimes B), \tag{21}$$

and respectively

$$f * g: A * B \to A * B, \quad (f * g)(x) := (f \otimes i)(x), \tag{21'}$$

we obtain a π-pair $(A * B, f * g)$

This construction (and a more general set up) will be discussed elsewhere (cf. [2]).

5. The classical case

Suppose now $R = \mathbb{Z}$ and consider the case $m = n = 2$. Start with an integer Δ and let $\mathbb{Z}_\Delta$ be the set of matrices $F \in \mathrm{Mat}(2; \mathbb{Z})$ satisfying

$$\operatorname{trace} F = 0 \quad \text{and} \quad \det F = -\Delta.$$

Hence $F^2 = \Delta \cdot I$ follows and $(\mathbb{Z}^2, F)$ is a Δ-pair. Let $M\{\Delta\}$ denote the subset of $\mathbb{Z}\{\Delta\}$ consisting of the equivalence classes

$$\mathfrak{a} = \{F\} := \{\mathbb{Z}^2, F\},$$

where $F \in \mathbb{Z}_\Delta$. Recall that $\{(F)\}$ depends only on the conjugacy class over $\mathbb{Z}$ of F.

PROPOSITION.

$M\{\Delta\}$ is a monoid under the composition $(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} * \mathfrak{b}$.

Proof. Put $\mathfrak{a} = \{F\}$ resp. $\mathfrak{b} = \{G\}$ and consider the $\mathbb{Z}$-module $C_{F,G}$ according to (14). Hence $C_{F,G}$ is a free $\mathbb{Z}$-module and $C_{F,G} \otimes \mathbb{C}$ has rank 2 over $\mathbb{C}$ in view of Proposition 3. Therefore the $\mathbb{Z}$-module $C_{F,G}$ has rank 2, too, and $\mathfrak{a} * \mathfrak{b}$ belongs to $M\{\Delta\}$. Clearly, the unit element $\mathfrak{e} = \{E\}$ (cf. (15)) belongs to $M\{\Delta\}$. □

Suppose that Δ is not a square in $\mathbb{Z}$, put $\Theta := \sqrt{\Delta}$ and consider the ring $\mathbb{Z}[\Theta]$. Let $\mathfrak{J} \neq \{0\}$ be an ideal in $\mathbb{Z}[\Theta]$. Then there exists $0 \neq a \in \mathbb{Z}^2$ and $F = F_{\mathfrak{J}} \in \mathbb{Z}_\Delta$ such that

$$\mathfrak{J} = \{a^t(F + \Theta I)g; g \in \mathbb{Z}^2\} \tag{22}$$

holds. Note that F is uniquely determined up to conjugation over $\mathbb{Z}$. Hence a mapping

$$\mathfrak{J} \mapsto \langle\!\langle F_{\mathfrak{J}} \rangle\!\rangle \tag{23}$$

of the ideals of $\mathbb{Z}[\Theta]$ into $M\{\Delta\}$ is well-defined. But $F_{\mathfrak{J}}$ depends only on the ideal class $\langle \mathfrak{J} \rangle$ of $\mathfrak{J}$ and consequently the mapping (23) induces a mapping ψ of the set $C(\Delta)$ of ideal classes of $\mathbb{Z}[\Theta]$ into $M\{\Delta\}$, which is bijective according to a classical result of R Dedekind (cf. [1], §187).

Clearly, the product $\mathfrak{J}_1\mathfrak{J}_2$ of two ideals $\mathfrak{J}_1, \mathfrak{J}_2$ of $\mathbb{Z}[\Theta]$ induces a product $\langle \mathfrak{J}_1 \rangle \langle \mathfrak{J}_2 \rangle := \langle \mathfrak{J}_1 \mathfrak{J}_2 \rangle$ of the corresponding ideal classes. Hence $C(\Delta)$ is a commutative monoid.

Lemma. The mapping $\psi: C(\Delta) \to M\{\Delta\}$ is an isomorphism.

Proof. Let $\mathfrak{J}_1$ and $\mathfrak{J}_2$ be non-zero ideals of $\mathbb{Z}[\Theta]$. Hence there exist $a, b \in \mathbb{Z}^2 \setminus \{0\}$ and $F, G \in \mathbb{Z}_\Delta$ such that

$$\mathfrak{J}_1 = \{a^t(F + \Theta I)g; g \in \mathbb{Z}^2\} \quad \text{resp.} \quad \mathfrak{J}_2 = \{b^t(G + \Theta I)h; h \in \mathbb{Z}^2\}$$

in view of (22). The elements of $\mathfrak{J}_1\mathfrak{J}_2$ are spanned by elements of the form

$$a^t(F + \Theta I)gh^t(G^t + \Theta I)b, \quad \text{where} \quad g, h \in \mathbb{Z}^2,$$

hence equal

$$a^t X_M b, \quad \text{where} \quad X_M := (F + \Theta I)M(G^t + \Theta I)$$

and where $M \in \mathrm{Mat}(2; \mathbb{Z})$. But one has

$$X_M = (FMG^t + \Delta M) + \Theta(FM + MG^t) = (F + \Theta I)Y_M,$$

where $Y_M := FM + MG^t$ holds. The use of (14) leads to

$$\mathfrak{J}_1\mathfrak{J}_2 = \{a^t(h(Y) + \Theta Y)b;\ Y \in C_{F,G}\},$$

where $\langle\!\langle C_{F,G}, h \rangle\!\rangle = \langle\!\langle F \rangle\!\rangle * \langle\!\langle G \rangle\!\rangle$. Now choose a basis of $C_{F,G}$ and compute

$$\mathfrak{J}_1\mathfrak{J}_2 = \{c^t(H + \Theta I)g; g \in \mathbb{Z}^2\}$$

for some $c \in \mathbb{Z}^2$ and $H \in \mathrm{Mat}(2; \mathbb{Z})$ such that $\langle\!\langle C_{F,G}, h \rangle\!\rangle = \langle\!\langle H \rangle\!\rangle$. □

Note that $C(\Delta)$ and hence $M\{\Delta\}$ in general fail to be groups, because $\mathbb{Z}[\Theta]$ in general fails to be the maximal order of the quadratic field $\mathbb{Q}[\Theta]$. However, $M\{\Delta\}$ acts on $\mathbb{Z}\{\Delta\}$ in view of Lemma 2.

In addition, using the map

$$S \mapsto JS, \quad \text{where} \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

from the set of symmetric 2×2 matrices over $\mathbb{Z}$ of determinant-Δ onto $\mathbb{Z}_\Delta$ the composition of integral binary quadratic forms in the sense of C F Gauss is mapped onto the product in $M\{\Delta\}$.

6. The $\mathbb{Z}$-module $D_{F,G}$

Suppose that the integer Δ is not a square. Given $F \in \mathrm{Mat}(m;\mathbb{Z})$ resp. $G \in \mathrm{Mat}(n;\mathbb{Z})$ satisfying

$$F^2 = \Delta \cdot I \quad \text{resp.} \quad G^2 = \Delta \cdot I,$$

consider the $\mathbb{Z}$-modules $C_{F,G}$ (cf. (14)) and

$$D_{F,G} = \{N \in \mathrm{Mat}(m,n;\mathbb{Z}); FN = NG^t\}. \tag{24}$$

Hence

$$C_{F,G} \subset D_{F,G} \tag{25}$$

holds according to (14').

PROPOSITION.

The $\mathbb{Z}$-modules $C_{F,G}$ and $D_{F,G}$ have the same rank.

Proof. Since $C := C_{F,G}$ and $D := D_{F,G}$ are free $\mathbb{Z}$-modules, it suffices to prove that the $\mathbb{C}$-ranks of $\mathbb{C} \otimes C$ and $\mathbb{C} \otimes D$ coincide. Without restriction assume $F \sim F_{p,q}$ resp. $G \sim F_{r,s}$, where $F_{p,q}$ is given by (16). Hence a computation leads to $\mathbb{C} \otimes C = \mathbb{C} \otimes D$. □

COROLLARY.

The index $i_{F,G}$ of $C_{F,G}$ in $D_{F,G}$ is finite.

Now consider a matrix

$$H := \begin{pmatrix} F & N \\ 0 & -G^t \end{pmatrix}, \tag{26}$$

where $N \in \mathrm{Mat}(m,n;\mathbb{Z})$. A computation leads to

$$N \in D_{F,G} \Leftrightarrow H^2 = \Delta \cdot I \tag{27}$$

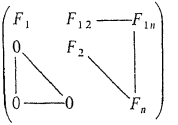
and to

$$\begin{pmatrix} I & M \\ 0 & I \end{pmatrix} H \begin{pmatrix} I & -M \\ 0 & I \end{pmatrix} = \begin{pmatrix} F & N - (FM + MG^t) \\ 0 & -G^t \end{pmatrix}. \tag{28}$$

Lemma. The number of conjugacy classes of matrices (26) satisfying $H^2 = \Delta \cdot I$ does not exceed $i_{F,G}$.

Proof. The matrices N in (26) can be reduced modulo $C_{F,G}$ according to (28). □

This result can be extended to arbitrary matrices $M \in \mathrm{Mat}(m; \mathbb{Z})$ satisfying $M^2 = \Delta \cdot I$, because M is conjugate to a matrix of the form



$$\begin{pmatrix} F_1 & F_{12} & \cdots & F_{1n} \\ 0 & F_2 & & \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & F_n \end{pmatrix} \tag{29}$$

where $m = 2n$ and where all F_i's belong to $\mathbb{Z}_\Delta$ and where all F_{ij}'s belong to $\mathrm{Mat}(2; \mathbb{Z})$ according to Theorem III.12 in [3]. Since $F_{ij} \in D_{F,G}$ holds, where $F := F_i$ and $G := -F_j^t$, the matrices F_{ij} can be reduced modulo $C_{F,G}$. In particular, *suppose that* $C_{F,G} = D_{F,G}$ *holds for all* $F, G \in \mathbb{Z}_\Delta$. *Then every* $M \in \mathrm{Mat}(m; \mathbb{Z})$ *satisfying* $M^2 = \Delta \cdot I$ *is over* $\mathbb{Z}$ *conjugate to a block diagonal matrix with diagonal blocks from* $\mathbb{Z}_\Delta$.

Given $F, G \in \mathbb{Z}_\Delta$,

$$F = \begin{pmatrix} f_1 & f_2 \\ f_3 & -f_1 \end{pmatrix}, \quad G = \begin{pmatrix} g_1 & g_2 \\ g_3 & -g_1 \end{pmatrix},$$

let

$$e_{F,G} := gcd(f_1 + g_1, f_1 - g_1, f_2, g_2, f_3, g_3).$$

Without proof we mention that

$$C_{F,G} = e_{F,G} \cdot D_{F,G}$$

holds. In particular, $e_{F,G} = 1$ for $F, G \in \mathbb{Z}_\Delta$, whenever Δ is square free and $\Delta \not\equiv 1 \pmod 4$.

References

[1] Dirichlet P G L and Dedekind R, *Vorlesungen über Zahlentheorie*, Vieweg (1894)
[2] Koecher M, On endomorphisms satisfying a given polynomial identity (to appear)
[3] Newman M, Integral matrices (New York: Academic Press) (1972)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 189–199.
© Printed in India.

Traces of Eichler–Brandt matrices and type numbers of quaternion orders

OTTO KÖRNER
Abteilung für Mathematik IV der Universität, Oberer Eselsberg, D 7900 Ulm, FRG

Abstract. Let A be a totally definite quaternion algebra over a totally real algebraic number field F and M be the ring of algebraic integers of F. For any M-order G of A we derive formulas for the mass $m(G)$ and the type number $t(G)$ of G and for the trace of the Eichler–Brandt matrix $B(G, J)$ of G and any integral ideal J of M in terms of genus invariants of G and of invariants of F and J. Applications to class numbers of quaternion orders and of ternary quadratic forms are indicated.

Keywords. Quaternion orders; class numbers; Eichler–Brandt matrices.

1. Introduction

Let $F, M, A, G, m(G), t(G)$ and $B(G, J)$ be as in the abstract above (s. definitions of these concepts in the following sections). The formulas for $m(G)$ (s. Theorem 1) and for the trace $\operatorname{Tr} B(G, J)$ (s. Theorem 2) and for $t(G)$ (s. Theorem 3) we derive in this paper generalize results that were obtained by Eichler [2], Peters [10] and Pizer [11], [12] for M-orders G of special type. For general G some of our results were stated without proof in [8]. Similarly as Pizer [11] we use for our proofs integration on some quotient spaces of the idele group of A and an elementary version of Selberg's trace formula (s. Lemma 2). It is clear that the results can be applied to the computation of the class number $h(G)$ of G because of the relation $h(G) = \operatorname{Tr} B(G, M)$. An application to any totally definite ternary quadratic M-lattice L is as follows. The second Clifford algebra C_2 of the quadratic F-vector space $F \otimes_M L$ is a totally definite quaternion algebra over F. Consider the M-order O_L of C_2 corresponding to L in the sense of Eichler [3], § 14. Then the type number $t(O_L)$ equals the number of all classes in the genus of L, as can be seen by deductions analogous to [10].

2. Notations, definitions and known consequences

By $|S|$ we denote the cardinality of any set S. For any ring R with unit element we denote the multiplicative group of all units of R by $U(R)$.

First, more generally than in the introduction, let F be the quotient field of any Dedekind domain M and A be a separable finite dimensional F-algebra. Subalgebras (e.g. F) of A are supposed to have the same unit element as A. Denote by P the set of all maximal ideals of M. If $p \in P$, then the spot of F corresponding to p is also denoted by p. An M-lattice on A is defined to be a finitely generated submodule of

the M-module A containing an F-basis of A. An M-order of A is by definition an M-lattice on A containing M and being a subring of A. For any M-lattice Λ on A the sets $\Lambda^{(l)} = \{x \in A \mid x\Lambda \subset \Lambda\}$ and $\Lambda^{(r)} = \{x \in A \mid \Lambda x \subset \Lambda\}$ are M-orders of A. Let G be any M-order of A. Then an M-lattice Λ on A with $G \subset \Lambda^{(l)}$ or $G \subset \Lambda^{(l)} \cap \Lambda^{(r)}$ is called a left ideal or a two-sided ideal of G respectively. A left ideal Λ of G is called invertible, if $\Lambda\Lambda^{-1} = G$, where $\Lambda^{-1} = \{x \in A \mid \Lambda x\Lambda \subset \Lambda\}$; Λ is called integral, if $\Lambda \subset G$; it is called primitive, if Λ is integral, invertible and not contained in pG for all $p \in P$.

Now let F be an algebraic number field or the completion of such a field at a discrete spot, and let M be the ring of integers of F. For any spot p of F (not necessarily in P) we denote by F_p the completion of the field F at p and by A_p the topological F_p-algebra being the completion of A with respect to the p-adic topology. Denote by P_o the set of all spots p of F for which A_p is a skew field. If S is a subset of A, then let S_p denote its closure in A_p. If $p \in P$, then $U(A_p)$ is an open subset of A_p and (with respect to the subset topology) a locally compact group with a countable basis for its topology, and $U(G_p)$ is an open compact subgroup. In the following Π always means the product over all $p \in P$. The restricted idele group $\hat{U}(A)$ of A is a subgroup of $\Pi U(A_p)$ and defined to be the union of all sets of the form $T = \Pi T^{(p)}$, where $T^{(p)}$ is any open subset of $U(A_p)$ such that $T^{(p)} = U(G_p)$ for almost all p (i.e. for all but finitely many); and the sets T are to form a basis for the (open sets of the) topology of $\hat{U}(A)$. This way $\hat{U}(A)$ becomes a topological group whose definition is independent of the choice of the order G, since for any other M-order G' of A one has $G'_p = G_p$ for almost all p by the Local–Global Principle for M-lattices [9]. The group $\hat{U}(A)$ is locally compact and has a countable basis for its topology. The group $U(A)$ is viewed as a subgroup of $\hat{U}(A)$ by the diagonal embedding. If K is any subalgebra of A, then $\hat{U}(K)$ is regarded as a subgroup of $\hat{U}(A)$ by the canonical inclusion map. If Λ is an M-lattice on A and $x = (x_p) \in \hat{U}(A)$, then we denote by Λx the unique M-lattice on A satisfying $(\Lambda x)_p = \Lambda_p x_p$ for all $p \in P$. Analogously $x\Lambda$ is defined.

Additionally let A be F or a two-dimensional separable F-algebra or a quaternion algebra over F. Then it is known [6] that an M-lattice Λ on A is an invertible left ideal of G, if and only if $\Lambda = Gy$ for some $y \in \hat{U}(A)$. Two invertible left ideals Λ, Λ' of G are said to be in the same class, if $\Lambda' = \Lambda x$ for some $x \in U(A)$. The number $h(G)$ (possibly infinite) of the classes of all invertible left ideals of G is called the class number of G. Since $\Lambda = Gy$, $\Lambda' = Gy'$, $y, y' \in \hat{U}(A)$, we have Λ and Λ' in the same class, if and only if y' lies in the double coset $\hat{U}(G)yU(A)$, where $\hat{U}(G)$ denotes the subgroup $\Pi U(G_p)$ of $\hat{U}(A)$. Hence $h(G)$ equals the cardinality of the set $\hat{U}(G)\backslash\hat{U}(A)/U(A)$ of all double cosets. Since $\hat{U}(M) = \Pi U(M_p)$ is a subgroup of $\hat{U}(G)$ and of the centre of $\hat{U}(A)$, the canonical homomorphism $k: \hat{U}(A) \to \hat{U}(A)/\hat{U}(M)$ yields

$$h(G) = |\hat{U}(G)\backslash\hat{U}(A)/U(A)| = |k(\hat{U}(G))\backslash k(\hat{U}(A))/k(U(A))|. \tag{1}$$

Additionally let $A \neq F$. Then we denote by $T(x) = x + x^*$ the reduced trace and by $N(x) = xx^*$ the reduced norm of any $x \in A$, where $x \mapsto x^*$ is the standard involution of A. The norm $N(\Lambda)$ of any M-lattice Λ on A is defined to be the submodule of the M-module F generated by the reduced norms of all elements of Λ. Apparently $N(\Lambda)$ is a fractional ideal of M (i.e. an M-lattice on F). We denote by $v(G)$ the set of the norms of all primitive two-sided ideals of G.

From now on let F, M, A and G be as in the introduction. That A be totally definite means that all archimedian spots of F belong to P_o, in other words: $N(x)$ is a totally

positive number in F for all non-zero $x \in A$. The reduced discriminant $d_r(G)$ of G is defined to be the integral ideal of M satisfying $(d_r^2(G))_p = M_p \det(T(x_{ip}x_{jp}^*))$ for all $p \in P$, where $x_{1p}, \ldots, x_{4p}$ is any M_p-basis of G_p. In the Theorems 1–3 and their proofs Π' means always the product over all $p \in P$ satisfying $p | d_r(G)$.

3. Tools from integration on groups

The following elementary lemma (whose proof is obvious) is convenient for proving the finiteness of class numbers.

Lemma 1. Let D be a discrete subgroup of a locally compact group L and B be an open compact subgroup of L. Then the set $B \backslash L/D$ is finite, if and only if the homogeneous space L/D is compact.

Let D, L, B be as in Lemma 1 and suppose that L/D is compact and that L has a countable basis for its topology. Then D as a discrete subgroup of L is countable (possibly finite), and L is unimodular. Denote by μ the left invariant Haar measure on L with $\mu(B) = 1$. That L is unimodular means that μ is also right invariant. For any $s \in D$ let $D(s)$ denote the centralizer of s in D, and μ_s be the L-left invariant quotient measure of μ on $L/D(s)$ normalized by the condition

$$\int_L f(x)\,\mathrm{d}\mu(x) = \int_{L/D(s)} \left(\sum_{g \in D(s)} f(xg) \right) \mathrm{d}\mu_s(xD(s)) \tag{2}$$

for every complex-valued continuous function f on L with compact support. A consequence of (2) is

$$\mu_s(BxD(s)/D(s)) = |x^{-1}Bx \cap D(s)|^{-1} \tag{3}$$

for all $x \in L$. Under the conditions for D, L, B assumed as above one has

Lemma 2. Let Bx_iD $(i = 1, \ldots, H)$ be the different double cosets with $x_i \in L$, and let f be a complex-valued continuous function on L, with compact support such that $f(b_1xb_2) = f(x)$ for all $x \in L$, $b_1, b_2 \in B$. Then in the series $R(x) = \sum_{g \in D} f(xgx^{-1})$ almost all terms vanish, if the variable x is restricted to any compact subset of L. Furthermore

$$\sum_{i=1}^{H} |x_i^{-1}Bx_i \cap D|^{-1} R(x_i) = \sum_{s \in S} I_s, \tag{4}$$

where

$$I_s = \int_{L/D(s)} f(xsx^{-1})\,\mathrm{d}\mu_s(xD(s))$$

and S denotes any fixed system of representatives for the conjugacy classes in D.

Proof. From Selberg's trace formula [13] it is possible to deduce (4); but for the convenience of the reader I prefer to present here an elementary direct proof. Since f has compact support and D is discrete, almost all terms of the series $R(x)$ vanish on every fixed compact subset of L. The series defines a continuous function on L/D

being constant of value $R(x_i)$ on each set Bx_iD/D. These sets form a disjoint covering of L/D. Therefore, if one denotes the left hand side of (4) by Γ, it follows from (3) that

$$\Gamma = \int_{L/D} R(x)\,\mathrm{d}\mu_1(xD) \quad (1 = \text{unit element of } D).$$

Denote by $M(s)$ any system of representatives for the cosets $gD(s)$ with $g \in D$. Then $R(x) = \sum_{s \in S} \sum_{g \in M(s)} f_s(xg)$ with the abbreviation $f_s(x) = f(xsx^{-1})$, and hence

$$\Gamma = \sum_{s \in S} J_s, \quad J_s = \int_{L/D} \left(\sum_{g \in M(s)} f_s(xg) \right) \mathrm{d}\mu_1(xD).$$

The substitution formula for integrals based on (2) shows that $J_s = I_s$, q.e.d.

4. Mass and Eichler–Brandt matrix

The finiteness of the class number $h(G)$ is evident from (1), Lemma 1 and the following lemma.

Lemma 3. (a) *The group index* $(U(G): U(M))$ *is finite.* (b) *The group* $k(\hat{U}(A))$ *is locally compact, has a countable basis for its topology and* $k(\hat{U}(G))$ *as an open compact subgroup and* $k(\hat{U}(A))$ *as a discrete subgroup. The homogeneous space* $k(\hat{U}(A))/k(U(A))$ *is compact.*

Proof. The group homomorphism $U(G) \to U(M)/(U(M))^2$, defined by $x \mapsto N(x)(U(M))^2$, has the kernel $U_1 U(M)$, where the set $U_1 = \{x \in G \mid N(x) = 1\}$ is finite, since A is totally definite. Hence $(U(G): U(M)) \leqslant |U_1|(U(M):(U(M))^2)$, where the last term is finite by the Dirichlet Unit Theorem. This proves (a). Since $\hat{U}(M)$ is a closed subgroup of $\hat{U}(A)$, the group $k(\hat{U}(A))$ is Hausdorff. Since $\hat{U}(A)$ is locally compact, has a countable basis and $\hat{U}(G)$ as an open compact subgroup, the corresponding images under k have the same properties. In order to prove that $k(U(A))$ is discrete, it suffices to show that its intersection with the open set $k(\hat{U}(G))$ is finite. This intersection equals $k(\hat{U}(G) \cap U(A)) = k(U(G)) \cong U(G)/(U(G) \cap \hat{U}(M)) = U(G)/U(M)$, and this is finite by (a). If G is a maximal M-order of A, then $h(G)$ is known to be finite [1], hence $k(\hat{U}(A))/k(U(A))$ is compact by (1) and Lemma 1, q.e.d.

Let $G_1, \ldots, G_h$ $(h = h(G))$ be any system of representatives for the classes of all invertible left ideals of G. Then the mass $m(G)$ of G is defined by

$$m(G) = \sum_{i=1}^{h} (U(G_i^{(r)}): U(M))^{-1}.$$

This is independent of the choice of the representatives G_i, as is clear e.g. by the following theorem.

Theorem 1. *One has*

$$m(G) = \frac{2D_F^{3/2} h_F \zeta_F(2)}{(2\pi)^{2n}} N_a(d_r(G)) \prod{}' \frac{1 - N_a(p)^{-2}}{1 - (G_p/p) N_a(p)^{-1}};$$

here D_F is the absolute discriminant, h_F the class number, n the degree, $\zeta_F(\ )$ the Dedekind zetafunction of the number field F, and $N_a(\ )$ means taking the absolute norm of ideals of M, and (G_p/p) is the Eichler symbol of the M_p-order G_p of A_p as defined in [7].

Proof. We have $G_i = Ga_i$ with $a_i \in \hat{U}(A)$, hence $G_i^{(r)} = a_i^{-1} G a_i$. According to Lemma 3 we may apply (3) to the case $L = k(\hat{U}(A))$, $B = k(\hat{U}(G))$, $D = k(U(A))$. By (1) there is the disjoint union

$$L = \bigcup_{i=1}^{h} Bk(a_i)D, \tag{5}$$

hence from (3) it follows that $\mu_1(L/D) = \sum |k(a_i)^{-1} Bk(a_i) \cap D|^{-1}$.
Now

$$|k(a_i)^{-1} Bk(a_i) \cap D| = |k(\hat{U}(G_i^{(r)}) \cap U(A))| = |k(U(G_i^{(r)}))|$$

$$= (U(G_i^{(r)}) : U(G_i^{(r)}) \cap \hat{U}(M)) = (U(G_i^{(r)}) : U(M)),$$

hence $\mu_1(L/D) = m(G)$ with respect to the normalization $\mu(B) = 1$ of the Haar measure μ on L. Therefore, if G' is any maximal M-order of A containing G, we obtain $m(G) = m(G')(\hat{U}(G') : \hat{U}(G))$. Because of $(U(G'_p) : U(G_p)) = 1$ for all $p \nmid d_s(G)$ this becomes $m(G) = m(G')\Pi'(U(G'_p) : U(G_p))$. Inserting here the value of $m(G')$ obtained by Eichler [1] and the value of $(U(G'_p) : U(G_p))$ derived in [8], we arrive immediately at the assertion of Theorem 1, q.e.d.

Let $G_1, \ldots, G_h$ be as before. Then $G_i^{-1} G_1, \ldots, G_i^{-1} G_h$ is a system of representatives for the classes of all invertible left ideals of $G_i^{(r)}$. Let J be any integral ideal of M and denote by $\pi_{ij}(J)$ the number of all integral invertible left ideals of $G_i^{(r)}$ that are in the same class as $G_i^{-1} G_j$ and whose norms equal J. Following [2] we define the Eichler–Brandt matrix $B(G, J)$ of G and J to be the matrix $(\pi_{ij}(J))$. Its trace $\sum \pi_{ii}(J)$ is denoted by $\operatorname{Tr} B(G, J)$, in particular it follows that $\operatorname{Tr} B(G, M) = h(G)$.

We denote by R any system of representatives in the multiplicative group $U^+(M)$ of all totally positive units of M for the cosets of the subgroup $(U(M))^2$. According to the Dirichlet Unit Theorem R is finite. For a fractional ideal I of M and $\beta \in U(F)$ we denote by $C(I, \beta)$ the finite set consisting of all $\alpha \in I$ with $\alpha^2 - 4\beta \notin F_p^2$ for all $p \in P_0$. For each $\alpha \in C(I, \beta)$ we fix any algebraic number $x = x(\alpha, \beta)$ satisfying $x^2 - \alpha x + \beta = 0$. Then our result on the trace of Eichler–Brandt matrices is as follows.

Theorem 2. *Let J be any integral ideal of M. If $\operatorname{Tr} B(G, J) \neq 0$, then $J = \beta M$ for some totally positive $\beta \in M$ and*

$$\operatorname{Tr} B(G, J) = \delta_\beta m(G) + \sum_{\varepsilon, \mathfrak{Q}} E_G(\Omega) \frac{h(\Omega)}{2(U(\Omega) : U(M))}.$$

Here $\delta_\beta = 1$ or 0 according as J is the square of a principal ideal of M or not. The conditions for summation are: $\varepsilon \in R$, $\alpha \in C(M, \varepsilon\beta)$, and the sum is over the finitely many M-orders Ω of the quadratic field extension $F[x]$ of F satisfying $x = x(\alpha, \varepsilon\beta) \in \Omega$. There $h(\Omega)$ is the class number of Ω and $E_G(\Omega) = \Pi' E(\Omega_p, G_p)$, and $E(\Omega_p, G_p)$ is the number of the classes of all optimal embeddings $\Omega_p \to G_p$.

For numerical applications of Theorem 2 it remains to compute the embedding numbers $E(\Omega_p, G_p)$. For orders G of special type this has essentially been done by Eichler [2], Hijikata [5] and Pizer [12]. Before proving Theorem 2 we have to say something on the definition and general properties of the embedding numbers. Let K be any quadratic field extension of F and Ω be an M-order of K. We fix any $p \in P$. Then Ω_p is an M_p-order of the separable F_p-algebra K_p. An optimal embedding $\psi: \Omega_p \to G_p$ is by definition an F_p-algebra monomorphism $\psi: K_p \to A_p$ such that $G_p \cap \psi(K_p) = \psi(\Omega_p)$. We say that two optimal embeddings $\psi, \psi': \Omega_p \to G_p$ are in the same class, if there exists an element u of $U(G_p)$ with $\psi' = \tau_u \psi$, where τ_u denotes the inner automorphism $x \mapsto uxu^{-1}$ of A_p. We denote by $[\psi]$ the class of an optimal embedding ψ. The embedding number $E(\Omega_p, G_p)$ turns out to be finite by the next lemma (which is a slight generalization of results in [5]). In order to prove the finiteness one may assume that K_p is a subalgebra of the F_p-algebra A_p. Under this assumption one has

Lemma 4. (a) *An one-to-one correspondence between the classes of all optimal embeddings $\Omega_p \to G_p$ and the double cosets $U(G_p)aU(K_p)$ with $a \in U(A_p)$ and $a^{-1}G_p a \cap K_p = \Omega_p$ is given by the assignment $U(G_p)aU(K_p) \mapsto [\psi_a]$, where ψ_a denotes the restriction of the inner automorphism τ_a of A_p to K_p.* (b) *The number $E(\Omega_p, G_p)$ is finite. It equals* 1, *if $p \nmid d_r(G)$.*

Proof. Since every F_p-algebra monomorphism $K_p \to A_p$ can be extended to an inner automorphism of A_p by the Skolem–Noether Theorem [14], the assignment described above produces the classes of all optimal embeddings $\Omega_p \to G_p$. The assignment is also injective, since $[\psi_a] = [\psi_b]$ implies that $\psi_a = \tau_u \psi_b$ for some $u \in U(G_p)$, hence $a^{-1}ub$ commutes with all elements of K_p and therefore lies in $U(K_p)$ by Lemma 5 (s. below). This proves (a). Replacing G in the double cosets by any maximal M-order G' of A containing G shows that

$$E(\Omega_p, G_p) \leqslant (U(G'_p): U(G_p)) \sum E(\Omega', G'_p), \tag{6}$$

where the sum is over all M_p-orders Ω' of K_p containing Ω_p. The number of these Ω' is finite, because Ω' is determined by its conductor which divides the conductor of Ω_p. If $p \nmid d_r(G)$, then $E(\Omega_p, G_p) = 1$ by [5], Corollary 2.6. It remains to consider the case $p \mid d_r(G')$. Here it is known [2] that $(U(A_p): U(F_p)U(G'_p)) = 2$, hence $E(\Omega', G'_p) \leqslant 2$ by part (a), hence $E(\Omega_p, G_p)$ is finite by (6), q.e.d.

The following lemma is well known (for part (b) s.e.g. [11], Lemma 8).

Lemma 5. Let A_0 be a quaternion algebra over a field F_0 (the centre of A_0) of characteristic $\neq 2$ and let $x \in A_0$, $\alpha \in F_0$, $\alpha \neq 1$.
(a) *if $x \notin F_0$, then the centralizer of x in A_0 is $F_0[x]$.*
(b) *If $x \in U(A_0)$, then there exists an element y of $U(A_0)$ such that $yxy^{-1} = \alpha x$ if and only if $\alpha = -1$ and $T(x) = 0$.*

Proof of Theorem 2. We use all notations of the proof of Theorem 1. By definition $\pi_{ii}(J)$ equals the number of all sets $G_i^{(r)} x$ with $x \in G_i^{(r)}$ and $N(x)M = J$. We suppose that $\mathrm{Tr}\, B(G, J) \neq 0$. Then $J = \beta M$ for some totally positive $\beta \in M$. On L we define a function f as follows. Let $y \in \hat{U}(A)$. Put $f(k(y)) = 1$, if $y_p \in G_p$ and $N(y_p)M_p = J_p$ for all $p \in P$.

Otherwise put $f(k(y)) = 0$. By Lemma 2 and (5), equation (4) holds for f with $x_i = k(a_i)$. Because of $G_i^{(r)} = a_i^{-1}Ga_i$ the term $R(x_i)$ equals the number of all cosets $x\hat{U}(M)$ with $x \in G_i^{(r)}$ and $N(x)M = J$, hence $R(x_i) = (U(G_i^{(r)}):U(M))\pi_{ii}(J)$. On the other hand $(U(G_i^{(r)}):U(M)) = |x_i^{-1}Bx_i \cap D|$ by the proof of Theorem 1. Therefore $\mathrm{Tr}\, B(G, J)$ equals the left hand side of (4). It remains to evaluate the integrals I_s on the right hand side of (4) and to describe the set S. We write $s = k(x)$ for some $x \in U(A)$ and distinguish the following two cases.

Case 1: $x \in U(F)$.
Here $I_s = f(s)\mu_1(L/D)$. Since $\mu_1(L/D) = m(G)$ by the proof of Theorem 1, we obtain $I_s = m(G)$ or 0, according as $x^2M = J$ or not.

Case 2: $x \notin U(F)$.
We put $K = F[x]$ and $D'(s) = k(U(K))$. By Lemma 5 the group index $t_s = (D(s):D'(s))$ satisfies $t_s = 2$ or 1, according as $T(x) = 0$ or not. It follows that

$$I_s = t_s^{-1} I'_s, \quad I'_s = \int_{L/D'(s)} f(ysy^{-1})\, \mathrm{d}\mu'_s(yD'(s)), \tag{7}$$

where μ'_s is the L-left invariant quotient measure of μ on the compact homogeneous space $L/D'(s)$ normalized by the condition $\mu'_s(L/D'(s)) = t_s\mu_s(L/D(s))$. The integral I'_s is non-zero, if and only if $N(x)M = J$ and $x \in y_0^{-1}Gy_0$ for some $y_0 \in \hat{U}(A)$, in particular

$$x^2 - \alpha x + \varepsilon\beta = 0 \tag{8}$$

for some $\alpha \in M$ and $\varepsilon \in U^+(M)$ with $\alpha^2 - 4\varepsilon\beta \notin F_p^2$ for all $p \in P_0$, since K_p is a subfield of A_p for all $p \in P_0$. Under the condition (8) we have $I'_s = \mu'_s(\cup W(y))$, where $W(y) = Bk(y\hat{U}(K))/D'(s)$ and the union $\cup$ is over all $y \in \hat{U}(A)$ with $x \in y^{-1}Gy$. Different sets of $W(y)$ are disjoint because of $D'(s) \subset k(\hat{U}(K))$. The condition $x \in y^{-1}Gy$ implies that $\Omega = y^{-1}Gy \cap K$ is an M-order of K containing x. If Ω is kept fixed, we denote by $W(y_j)$ $(j = 1, \ldots, E(\Omega))$ the different sets among the $W(y)$ with $y^{-1}Gy \cap K = \Omega$. Then $E(\Omega)$ is the number of double cosets $\hat{U}(G)z\hat{U}(K)$ with $z \in \hat{U}(A)$ and $z_p^{-1}G_pz_p \cap K_p = \Omega_p$ for all $p \in P$. By Lemma 4 it follows that $E(\Omega) = E_G(\Omega)$. Denote by $G^{(j)}$ the M-order $y_j^{-1}Gy_j$ of A. Then $\mu'_s(W(y_j)) = \mu'_s(k(\hat{U}(G^{(j)})\hat{U}(K))/D'(s))$ by the left invariance of μ'_s, hence

$$I'_s = \sum_{\Omega, j} \mu'_s(k(\hat{U}(G^{(j)})\hat{U}(K))/D'(s)),$$

where the sum is over all M-orders Ω of K containing x and over $j = 1, \ldots, E_G(\Omega)$. Since $h(\Omega) = (\hat{U}(K):\hat{U}(\Omega)U(K))$ by (1), we have for each Ω the disjoint union

$$\hat{U}(K) = \bigcup_{\rho} \hat{U}(\Omega)U(K)\beta_\rho$$

for some $\beta_\rho \in \hat{U}(K)$, where $\rho = 1, \ldots, h(\Omega)$, hence

$$\hat{U}(G^{(j)})\hat{U}(K) = \bigcup_{\rho} \hat{U}(G^{(j)})U(K)\beta_\rho. \tag{9}$$

This union is also disjoint, since $\beta_\sigma \in \hat{U}(G^{(j)})U(K)\beta_\rho$ implies $\beta_\sigma\beta_\rho^{-1} \in (U(G^{(j)}) \cap \hat{U}(K))U(K) =$

$\hat{U}(\Omega)U(K)$. Because of $D'(s)=k(U(K))$ the application of the canonical map $\hat{U}(A)\to L/D'(s)$ to (9) yields again a disjoint union, hence

$$I'_s=\sum_{\Omega,j,\rho}\mu'_s(k(\hat{U}(G^{(j)})\beta_\rho)D'(s)/D'(s)), \tag{10}$$

where the conditions of summation for Ω, j, ρ are as before. We denote by $G^{(j,\rho)}$ the M-order $\beta_\rho^{-1}G^{(j)}\beta_\rho$ of A and put $B_{j\rho}=k(\hat{U}(G^{(j,\rho)}))$. Then $\mu(B_{j\rho})=\mu(B)=1$, since μ is left and right invariant. The left invariance of μ'_s implies $\mu'_s(k(\hat{U}(G^{(j)})\beta_\rho)D'(s)/D'(s))=\mu'_s(B_{j\rho}D'(s)/D'(s))$, and this equals $|B_{j\rho}\cap D'(s)|^{-1}$ by the analogue of (3) and because of $\mu(\beta_{j\rho})=1$. Furthermore $|B_{j\rho}\cap D'(s)|=|k(\hat{U}(G^{(j,\rho)})\cap U(K))|=|k(\hat{U}(G^{(j)})\cap U(K))|=|k(U(\Omega))|=(U(\Omega):U(M))$. Therefore it follows from (10) and (7) that

$$I_s=t_s^{-1}\sum_{\Omega}E_G(\Omega)h(\Omega)/(U(\Omega):U(M)), \tag{11}$$

where the sum is over all M-orders Ω of $F[x]$ containing x. Note that any quadratic field extension $F[y]$ of F, where y is any root of equation (8), can be embedded as F-algebra in the F-algebra A (s. [14], page 78). Therefore (11) remains valid, if x is replaced by such y. Now we describe a system S (as needed in (4)) of representatives for the conjugacy classes in D. In Case 1 different elements s represent different conjugacy classes. Consequently the contribution of Case 1 to $\operatorname{Tr}B(G,J)$ is $\delta_\beta m(G)$. In Case 2 elements $s=k(x)$, $s'=k(x')$ with $x,x'\in U(A)-U(F)$ represent the same conjugacy class if and only if ηx and x' are conjugate in $U(A)$ for some $\eta\in U(M)$. By the Skolem–Noether Theorem [14] this amounts to the conditions $T(\eta x)=T(x')$, $N(\eta x)=N(x')$. Therefore in Case 2 we may restrict ourselves to elements s of the form $s=k(x)$ with $T(x)=\alpha$, $N(x)=\varepsilon\beta$, $\varepsilon\in R$, $\alpha\in C(M,\varepsilon\beta)$. Then two elements $s=k(x)$, $s'=k(x')$ of this form are conjugate in D, if and only if $\varepsilon=\varepsilon'$, $\alpha=\pm\alpha'$, i.e. each conjugacy class is represented twice, except in the case $T(x)=0$, there only once. This and (11) show that Theorem 2 is true.

5. The type number

Two M-orders G, G' of A are said to be in the same genus, if G_p and G'_p are isomorphic as M_p-algebras for all $p\in P$. The orders G, G' are said to be in the same isomorphism class, if they are isomorphic as M-algebras. The type number $t(G)$ of G is defined as the number of all isomorphism classes in the genus of G. Let $\Gamma(G)$ be the normalizer of G in $U(A)$, i.e. the subgroup $\{x\in U(A)\mid xGx^{-1}=G\}$ of $U(A)$. Then the normalizer $\hat{\Gamma}(G)$ of G in $\hat{U}(A)$ equals $\hat{U}(A)\cap\Pi\Gamma(G_p)$, where $\Gamma(G_p)$ denotes the normalizer of G_p in $U(A_p)$. Since any isomorphism $G_p\cong G'_p$ or $G\cong G'$ can be extended to an inner automorphism of the corresponding quaternion algebra by the Skolem–Noether Theorem [14], the group $\hat{U}(A)$ acts via conjugation transitively on the genus of G and the group $U(A)$ acts via conjugation transitively on the isomorphism class of G, hence

$$t(G)=|\hat{\Gamma}(G)\backslash\hat{U}(A)/U(A)|. \tag{12}$$

From this and (1) it follows that $t(G)\leqslant h(G)$; in particular $t(G)$ is finite. For the sequel we shall need the group index $q:=(\hat{\Gamma}(G):\hat{U}(F)\hat{U}(G))$. Note that $(\Gamma(G_p):U(F_p)U(G_p))$ is

the cardinality of the central Picard group of G_p (s. [8]) and therefore finite [4] for all $p \in P$ and equal to 1 for $p \nmid d_r(G)$ (s. [2]). This implies

$$q = \Pi'(\Gamma(G_p): U(F_p)U(G_p)). \tag{13}$$

Since the factors of this product have been computed in [8], the index q is explicitly known. Furthermore we shall need the set $v(G)$ as defined in the second section. The Local–Global principle shows that $v(G)$ is the set of all integral ideals J of M such that $J_p \in v(G_p)$ for all $p \in P$. Each set $v(G_p)$ is finite and explicitly known [8]. Since $v(G_p) = \{M_p\}$ for $p \nmid d_r(G)$, the set $v(G)$ is also finite and known. With the same notations as in Theorem 2 we state

Theorem 3. *For any M-order G of A one has*

$$qh_F t(G) = m(G) + \sum_{\varepsilon, I, J} \sum_{\alpha, \Omega} E'_G(\Omega) \frac{h(\Omega)}{2(U(\Omega): U(M))}.$$

The sum is over all $\varepsilon \in R$, over all fractional ideals I of M in an arbitrarily fixed system of representatives for the ideal classes of M and over all integral ideals J of M satisfying $J \in v(G)$ and $I^2 J = \beta M$ for at least one totally positive $\beta \in F$. Having fixed such β for each J, one takes the second sum over all $\alpha \in C(I, \varepsilon\beta)$ and over all M-orders Ω of $F[x]$ with $x = x(\alpha, \varepsilon\beta)$ and $x \in I\Omega - pI\Omega$ for all $p \in P$. Here q is obtained by (13) *and $E'_G(\Omega) = \Pi' E'(\Omega_p, G_p)$, where $E'(\Omega_p, G_p)$ denotes the number of classes of all optimal embeddings $\psi: \Omega_p \to G_p$ satisfying $\psi(x) G_p = G_p \psi(x)$.*

For numerical applications of Theorem 3 it remains to compute the restricted embedding numbers $E'(\Omega_p, G_p)$. For special orders G this can be achieved by using results of [5], [10], [11], [12].

Proof of Theorem 3. Again we use all notations of the proof of Theorem 1. The group $\hat{U}(A)$ is the union of the double cosets $\hat{\Gamma}(G) a_i U(A)$. Such a double coset is the disjoint union of finitely many, say t_i, double cosets of the form $\hat{U}(G) c a_i U(A)$ with $c \in \hat{\Gamma}(G)$. Since $a_i^{-1} G a_i = G_i^{(r)}$ and $\hat{U}(G)$ is a normal subgroup of $\hat{\Gamma}(G)$, we obtain for c the condition $a_i^{-1} c a_i \hat{U}(G_i^{(r)}) U(A) \subset \hat{\Gamma}(G_i^{(r)}) U(A)$, hence $t_i = (\hat{\Gamma}(G_i^{(r)}) U(A): \hat{U}(G_i^{(r)}) U(A))$, and this term we denote by $g(G_i^{(r)})$. Since $\hat{U}(A)$ is the disjoint union of the double cosets $\hat{U}(G) a_i U(A)$, we see from (12) that

$$t(G) = \sum_{i=1}^{h} (g(G_i^{(r)}))^{-1},$$

where

$$g(G) = (\hat{\Gamma}(G): \hat{\Gamma}(G) \cap \hat{U}(G) U(A)) = (\hat{\Gamma}(G): \hat{U}(G) \Gamma(G))$$

$$= \frac{q(\hat{U}(F)\hat{U}(G): U(F)\hat{U}(G))}{(\hat{U}(G)\Gamma(G): U(F)\hat{U}(G))} = \frac{q(\hat{U}(F): \hat{U}(F) \cap U(F)\hat{U}(G))}{(\Gamma(G): \Gamma(G) \cap U(F)\hat{U}(G))}$$

$$= \frac{q(\hat{U}(F): U(F)\hat{U}(M))}{(\Gamma(G): U(F)U(G))} = \frac{qh_F}{(\Gamma(G): U(F)U(G))},$$

hence

$$qh_F t(G) = \sum_{i=1}^{h} (\Gamma(G_i^{(r)}): U(F)U(G_i^{(r)})). \tag{14}$$

We fix any system $\{C_\rho | \rho = 1, \ldots, h_F\}$ of representatives for the ideal classes of M. In particular we have $C_\rho = \gamma_\rho M$ for some $\gamma_\rho \in \hat{U}(F)$. For $x \in \Gamma(G)$ the set Gx is a two-sided ideal of G, hence $Gx = \alpha C_\rho \Lambda$ with $\alpha \in U(F)$, some primitive two-sided ideal Λ of G and some ρ. The pair ρ, Λ is uniquely determined by the coset $xU(F)U(G)$, and conversely. Therefore

$$(\Gamma(G) : U(F)U(G)) = \sum_\rho \sigma_\rho(G),$$

where $\sigma_\rho(G)$ denotes the number of all sets of the form $Gx = C_\rho \Lambda$ with $x \in U(A)$ and a primitive two sided ideal Λ of G; in particular $N(x)M = C_\rho^2 J$ for some $J \in \nu(G)$. We denote by $\hat{\Gamma}_0(G)$ the set of all $y \in \hat{\Gamma}(G)$ satisfying $y_p \in G_p - pG_p$ for all $p \in P$. Then $\{Gy | y \in \hat{\Gamma}_0(G)\}$ is the set of all primitive two-sided ideals of G. Therefore from (14) it follows that

$$q h_F t(G) = \sum_{\rho, J} S_\rho(J), \tag{15}$$

where the sum is over $\rho = 1, \ldots, h_F$ and over all $J \in \nu(G)$ and where

$$S_\rho(J) = \sum_{i=1}^{h} q_i(\rho, J)$$

and $q_i(\rho, J)$ denotes the number of all sets $G_i^{(\rho)} x$ with $x \in U(A) \cap \gamma_\rho \hat{\Gamma}_0(G_i^{(\rho)})$ and $N(x)M = C_\rho^2 J$. Now for any fixed ρ we compute the sum $S_\rho(J)$ by the method that we used for the evaluation of $\mathrm{Tr}\, B(G, J)$ in the proof of Theorem 2. For this we define a function f on L as follows. Let $y \in \hat{U}(A)$. Put $f(k(y)) = 1$, if $y \in \gamma_\rho \hat{\Gamma}_0(G)$ and $N(y_p)M_p = C_{\rho p}^2 J_p$ for all $p \in P$. Otherwise put $f(k(y)) = 0$. By Lemma 2 and (5), equation (4) holds for f with $x_i = k(a_i)$. As in the proof of Theorem 2 it follows that $S_\rho(J)$ equals the left hand side of (4). We suppose that $S_\rho(J) \neq 0$. Then there exists a totally positive $\beta \in F$ with $C_\rho^2 J = \beta M$. For computation of the integrals l_s on the right hand side of (4) we write $s = k(x)$ with $x \in U(A)$ and distinguish two cases.

Case 1: $x \in U(F)$.
As in the proof of Theorem 2 we conclude that $I_s = m(G)$ or 0, according as $C_\rho = Mx$ and $J = M$ or not.

Case 2: $x \notin U(F)$.
We put $K = F[x]$ and $D'(s) = k(U(K))$ and obtain as in the proof of Theorem 2 equation (7), and in the case $I_s' \neq 0$ also equation (8), but now with the conditions

$$\varepsilon \in U^+(M), \quad \alpha \in C(C_\rho, \varepsilon\beta). \tag{16}$$

Under the conditions (8) and (16) we have $I_s' = \mu_s'(\cup W(y))$, where $W(y) = Bk(y\hat{U}(K))/D'(s)$ and the union $\cup$ is over all $y \in \hat{U}(A)$ with $x \in \hat{\Gamma}(y^{-1}Gy)$ and

$$x \in C_\rho \Omega - pC_\rho \Omega \quad \text{for all} \quad p \in P. \tag{17}$$

Here Ω denotes the M-order $y^{-1}Gy \cap K$ of the F-algebra K. If Ω is kept fixed and x satisfies (8), (16) and (17), we denote by $W(y_j)$ $(j = 1, \ldots, E'(\Omega))$ the different sets $W(y)$

with $y \in \hat{U}(A)$, $y^{-1}Gy \cap K = \Omega$ and $yxy^{-1} \in \hat{\Gamma}(G)$. Then we have $E'(\Omega) = \Pi E'(\Omega_p, G_p)$ by Lemma 4. For $p \nmid d_A(G)$ the element $z_p = \gamma_{\rho p}^{-1} x$ of $y_p^{-1} G_p y_p$ satisfies $N(z_p) M_p = J_p = M_p$, hence $z_p \in U(y_p^{-1} G_p y_p)$, hence $x \in \Gamma(y_p^{-1} G_p y_p)$, hence $E'(\Omega_p, G_p) = E(\Omega_p, G_p) = 1$ by Lemma 4. Therefore $E'(\Omega) = E'_G(\Omega)$. It is clear that from here on the evaluation of I_s and the construction of the system S can be carried out as in the proof of Theorem 2. This way we obtain for $S_\rho(J)$ an expression analogous to that for $\operatorname{Tr} B(G, J)$ in Theorem 2. Inserting this in (15) completes the proof of Theorem 3.

References

[1] Eichler M, Über die Klassenzahl total definiter Quaternionenalgebren, *Math. Z.* **43** (1937) 102–109
[2] Eichler M, Zur Zahlentheorie der Quaternionen algebren, *J. reine angew. Math.* **195** (1955) 127–151
[3] Eichler M, Quadratische Formen und orthogonale Gruppen 1974 2nd edn (Berlin: Springer Verlag)
[4] Fröhlich A, The Picard group of non-commutative rings, in particular of orders, *Trans. Am. Math. Soc.* **180** (1973) 1–45
[5] Hijikata H, Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$, *J. Math. Soc. Jpn.* **26** (1974) 56–82
[6] Kaplansky I, Submodules of quaternion algebras, *Proc. London Math. Soc.* (3) **19** (1969) 219–232
[7] Körner O, Ordnungen von Quaternionenalgebren über lokalen Körpern, *J. reine angew. Math.* **333** (1982) 162–178
[8] Körner O, Über die zentrale Picard-Gruppe und die Einheiten lokaler Quaternionenordnungen, *Manuscripta Math.* **52** (1985) 203–225
[9] O'Meara O T, Introduction to quadratic forms 1963 (Berlin: Springer-Verlag)
[10] Peters M, Ternäre und quaternäre quadratische Formen und Quaternionen algebren *Acta Arith.* **15** (1969) 329–365
[11] Pizer A, Type numbers of Eichler orders, *J. reine angew. Math.* **264** (1973) 76–102
[12] Pizer A, On the arithmetic of quaternion algebras, *Acta Arith.* **31** (1976) 61–89
[13] Tamagawa T, On Selberg's Trace Formula, *J. Fac. Sci. Univ. Tokyo, Sect. I* **8** (1960) 363–386
[14] Vignéras M F, Arithmétique des Algébres de Quaternions, *Lecture Notes in Mathematics* 800 (1980) (Berlin: Springer Verlag)

© Printed in India.

The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions

ALOYS KRIEG

Mathematisches Institut, Westfälische Wilhelms-Universität, Einsteinstr. 62, D-4400 Münster, Federal Republic of Germany

Abstract. In the present paper the elementary divisor theory over the Hurwitz order of integral quaternions is applied in order to determine the structure of the Hecke-algebras related to the attached unimodular and modular group of degree n. In the case $n = 1$ the Hecke-algebras fail to be commutative. If $n > 1$ the Hecke-algebras prove to be commutative and coincide with the tensor product of their primary components. Each primary component turns out to be a polynomial ring in n resp. $n + 1$ resp. $2n$ resp. $2n + 1$ algebraically independent elements. In the case of the modular group of degree n, the law of interchange with the Siegel ϕ-operator is described. The induced homomorphism of the Hecke-algebras is surjective except for the weights $r = 4n - 4$ and $r = 4n - 2$.

Keywords. Hecke-algebra; unimodular group; modular group; quaternions; Hurwitz order; Siegel ϕ-operator.

1. The abstract Hecke-algebra

1.1. *Introduction*

G Shimura [14], Chapter 3, introduced the notion of abstract Hecke-algebra and established the framework of all types of Hecke-algebras, which have been investigated up to now. Using the elementary divisor theory he determined the structure of the Hecke-algebra related to the unimodular group. In the case of the Siegel modular group the structure theorem was proved by G Shimura [13], whereas special cases are due to H Maaß [11]. Confer also E Freitag [3], Chapter 4, where moreover applications to Siegel modular forms are described.

T Tamagawa [16] considered the unique maximal order in a division algebra over the p-adic number field and investigated the structure of the Hecke-algebra related to the attached unimodular group.

Looking at a division algebra over a global field, the situation becomes more complicated. In the present paper we deal with the Hurwitz order of integral quaternions. Applying the associated elementary divisor theory, which was developed in [9] and [17], we can determine the structure of the Hecke-algebra related to the unimodular group of degree n, whenever $n > 1$. Then one can decompose the Hecke-algebra into its primary components and each primary component proves to be a polynomial ring. Additional considerations yield the structure theorem for the Hecke-algebra related to the modular group of quaternions, which was introduced in [7]. The corresponding law of interchange with the Siegel ϕ-operator yields a homomorphism of the algebras, which surprisingly fails to be surjective for two weights. For the sake of

completeness the Hecke-algebras related to the unimodular group over a principal ideal domain and related to the Hermitian modular group over an imaginary quadratic number field of class number one are included.

Although the results look similar to those in [3], [13], [14], [16], the proofs proceed in a different way. Especially we do not use induction on the degree n, because the Hecke-algebras over the Hurwitz order for $n=1$ become exceptional, namely non-commutative.

1.2. *Notation*

Let $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ resp. $\mathbb{C}$ denote the set of positive integral, non-negative integral, integral, rational, real resp. complex numbers and $\mathbb{H}$ the skew field of real Hamiltonian quaternions. If R is a unitary ring, then $A^{(m,n)}$ resp. $A \in \mathrm{Mat}(m,n;R)$ means that A is an $m \times n$ matrix over R. The case $m=n$ is abbreviated by $A^{(n)}$ resp. $A \in \mathrm{Mat}(n;R)$. Moreover $GL(n;R)$ stands for the group of units in the ring $\mathrm{Mat}(n;R)$. Let A' always denote the transpose of A. The letter I is reserved for the identity matrix and 0 for the zero-matrix of appropriate size. If $A_1,\ldots,A_n$ are square matrices, then $[A_1,\ldots,A_n]$ stands for the square matrix with $A_1,\ldots,A_n$ as its diagonal blocks and zeros otherwise. The cardinality of a set $\mathcal{S}$ is denoted by $\#\mathcal{S}$.

1.3. *Definition of the abstract Hecke-algebra*

We follow the description in [14] resp. [3]. Given a multiplicative group $\mathcal{G}$, consider a subgroup $\mathcal{S}$ and a monoid $\mathcal{M}$ such that $\mathcal{S} \subset \mathcal{M} \subset \mathcal{G}$. The notation "$M:\mathcal{S}\backslash\mathcal{M}$" resp. "$M:\mathcal{S}\backslash\mathcal{M}/\mathcal{S}$" means that M runs through a set of representatives of the right cosets $\mathcal{S}M$ resp. of the double cosets $\mathcal{S}M\mathcal{S}$ modulo $\mathcal{S}$ in $\mathcal{M}$.

We suppose that the pair $(\mathcal{S},\mathcal{M})$ satisfies the *Hecke-condition*, i.e. each double coset $\mathcal{S}M\mathcal{S}$, $M \in \mathcal{M}$, decomposes into finitely many right cosets modulo $\mathcal{S}$:

$$\#(\mathcal{S}\backslash\mathcal{S}M\mathcal{S}) < \infty \quad \text{for all } M \in \mathcal{M}. \tag{1}$$

Denote by $\mathcal{H}(\mathcal{S},\mathcal{M})$ the $\mathbb{Z}$-module having the double cosets $\mathcal{S}M\mathcal{S}$, $M \in \mathcal{M}$, as a basis. Thus $\mathcal{H}(\mathcal{S},\mathcal{M})$ consists of all formal finite linear combinations of the form

$$T := \sum_{M:\mathcal{S}\backslash\mathcal{M}/\mathcal{S}} t(\mathcal{S}M\mathcal{S})\mathcal{S}M\mathcal{S},$$

where $t(\mathcal{S}M\mathcal{S}) \in \mathbb{Z}$ and $t(\mathcal{S}M\mathcal{S}) \neq 0$ only for finitely many double cosets $\mathcal{S}M\mathcal{S}$. Given such a T one defines

$$\deg T := \sum_{M:\mathcal{S}\backslash\mathcal{M}} t(\mathcal{S}M\mathcal{S}) \in \mathbb{Z}.$$

Given $M, N \in \mathcal{M}$ choose coset decompositions $\mathcal{S}M\mathcal{S} = \bigcup_{\mu=1}^{m} \mathcal{S}M_\mu$, $m = \deg \mathcal{S}M\mathcal{S}$, $\mathcal{S}N\mathcal{S} = \bigcup_{\nu=1}^{n} \mathcal{S}N_\nu$, $n = \deg \mathcal{S}N\mathcal{S}$. We define the product

$$(\mathcal{S}M\mathcal{S})\cdot(\mathcal{S}N\mathcal{S}) := \sum_{L:\mathcal{S}\backslash\mathcal{M}/\mathcal{S}} t(M,N;L)\mathcal{S}L\mathcal{S} \in \mathcal{H}(\mathcal{S},\mathcal{M}), \tag{2}$$

where

$$t(M,N;L) := \#\{(\mu,\nu);\ \mathcal{S}M_\mu N_\nu = \mathcal{S}L\}.$$

The product (2) is linearly extended to $\mathscr{H}(\mathscr{S},\mathscr{M})$. Thus $\mathscr{H}(\mathscr{S},\mathscr{M})$ becomes an associative $\mathbb{Z}$-algebra with $\mathscr{S}$ as its identity element (cf. [14], Proposition 3.4). We call $\mathscr{H}(\mathscr{S},\mathscr{M})$ the *Hecke-algebra related to the pair* $(\mathscr{S},\mathscr{M})$.

2. The Hecke-algebra related to the unimodular group

Before we deal with the Hurwitz order, we recall the commutative case. G Shimura's results [14], Chapter 3.2, are stated in a slightly more general form.

2.1. *The case of a commutative principal ideal domain*

We consider a principal ideal domain R, i.e. R is a commutative ring with identity element 1 without any zero-divisors, where every ideal is principal. Let $\mathscr{E}$ denote the group of units in R. As usual $a,b\in R$ are called associate, if $a=\varepsilon b$ holds for some $\varepsilon\in\mathscr{E}$. Then

$$\mathscr{U}_n := GL(n;R)=\{U\in \mathrm{Mat}(n;R);\ \det U\in\mathscr{E}\}$$

is said to be the *unimodular group of degree n over R*. Consider the monoid

$$\mathscr{M}_n := \mathscr{M}(n;R):=\{A\in\mathrm{Mat}(n;R);\det A\neq 0\}$$

and for $0\neq a\in R$ the submonoid

$$\mathscr{M}_{n,a}:=\{A\in\mathrm{Mat}(n;R);\det A=\varepsilon a^l,\varepsilon\in\mathscr{E},l\in\mathbb{N}_0\}.$$

In the trivial case $n=1$ the Hecke-algebra $\mathscr{H}(\mathscr{U}_1,\mathscr{M}_1)=\mathscr{H}(\mathscr{E},R-\{0\})$ coincides with the semigroup algebra of $\mathscr{M}_1/\mathscr{U}_1$ over $\mathbb{Z}$.

The elementary divisor theory for R is pointed out in [12], Chapter II. In every right coset $\mathscr{U}_nA$, $A\in\mathscr{M}_n$, there exists a matrix in Hermite normal form according to [12], Theorem II.2. Hence it follows that in the case $n>1$ the pair $(\mathscr{U}_n,\mathscr{M}_n)$ fulfills the Hecke-condition if and only if R satisfies the finiteness condition

$$N(a):=\#(R/Ra)<\infty \quad \text{for } 0\neq a\in R.$$

Now one can apply the same arguments, which were used in [14], resp. one can adopt the proofs given for the more complicated case in the sequel in order to obtain

Theorem 1. *Let R be a principal ideal domain satisfying the finiteness condition. Then the Hecke-algebra $\mathscr{H}(\mathscr{U}_n,\mathscr{M}_n)$ is commutative and coincides with the tensor product of its primary components, i.e.*

$$\mathscr{H}(\mathscr{U}_n,\mathscr{M}_n)=\bigotimes_{\pi}\mathscr{H}(\mathscr{U}_n,\mathscr{M}_{n,\pi}),$$

where π runs through a set of non-associate primes in R. If π is any prime, then $\mathscr{H}(\mathscr{U}_n,\mathscr{M}_{n,\pi})$ equals the polynomial ring over $\mathbb{Z}$ in n elements

$$T_{n,l}(\pi):=\mathscr{U}_n[I^{(n-l)},\pi I^{(l)}]\mathscr{U}_n,\quad l=1,\dots,n,$$

which are algebraically independent. Especially $\mathscr{H}(\mathscr{U}_n,\mathscr{M}_n)$ does not contain any zero-

divisors. Moreover

$$\sum_{A:\mathscr{U}_n\backslash\mathscr{M}_{n,\pi}/\mathscr{U}_n}(\mathscr{U}_nA\mathscr{U}_n)N(\det A)^{-s}$$
$$=\left(\sum_{l=0}^{n}(-1)^lT_{n,l}(\pi)N(\pi)^{(1/2)l(l-1)-ls}\right)^{-1}$$

holds formally in s.

Of course the Hecke-algebra $\mathscr{H}(\mathscr{U}_n, GL(n;\mathbb{F}))$, where $\mathbb{F}$ is the field of fractions over R, can be treated in the same way. The corresponding structure can easily be derived from Theorem 1. Especially the Hecke-algebra related to the analogue of the modular group in characteristic p considered by A Weil [20] is contained in Theorem 1.

2.2. *The Hurwitz order*

Let $1, i, j, k$ be the canonical basis of the skew field $\mathbb{H}$ of Hamiltonian quaternions (cf. [6], pp. 95–98). Denote the canonical conjugation by $x\mapsto\bar{x}$. Given $x\in\mathbb{H}$ then $\mathrm{Re}(x):=\frac{1}{2}(x+\bar{x})$, $\mathrm{Re}(x)\in\mathbb{R}$, stands for its real part and $N(x):=x\bar{x}\in\mathbb{R}$ for its norm.

Define $\rho:=\frac{1}{2}(1+i+j+k)$, then the $\mathbb{Z}$-module

$$\mathcal{O}:=\mathbb{Z}\rho+\mathbb{Z}+\mathbb{Z}i+\mathbb{Z}j$$

is called the *Hurwitz order* of integral quaternions. $\mathcal{O}$ is a maximal order in the rational quaternion algebra $\mathbb{Q}+\mathbb{Q}i+\mathbb{Q}j+\mathbb{Q}k$ and its arithmetical properties were investigated by A Hurwitz [5]. Note that $a\in\mathcal{O}$ implies

$$2\,\mathrm{Re}(a)\in\mathbb{Z}\quad\text{and}\quad N(a)\in\mathbb{N}_0.$$

$\mathcal{O}$ carries the structure of a non-commutative Euclidean ring.

The group $\mathscr{E}$ of units of $\mathcal{O}$ consists of 24 elements. The multiplicative monoid

$$\mathrm{Inv}\,\mathcal{O}=\{a\in\mathcal{O}-\{0\};a\mathcal{O}=\mathcal{O}a\}$$

of invariant elements was determined by A Hurwitz [5], Vorlesung 5, namely

$$\mathrm{Inv}\,\mathcal{O}=\{m\varepsilon;m\in\mathbb{N},\varepsilon\in\mathscr{E}\}\cup\{m(1+i)\varepsilon;m\in\mathbb{N},\varepsilon\in\mathscr{E}\}.$$

We state the notions of divisibility just as in [9]. Given $a,b\in\mathcal{O}-\{0\}$ set

$$a|_lb\text{ if }a^{-1}b\in\mathcal{O},\quad a|_rb\text{ if }ba^{-1}\in\mathcal{O},$$
$$a|b\text{ if }a|_lb\quad\text{and}\quad a|_rb.$$

If a or b is an invariant element, then $a|_lb$ and $a|_rb$ are equivalent in view of [7], I.1.12.

Each $0\neq a\in\mathcal{O}$ possesses a unique representation

$$a=(1+i)^enb,$$

where $e\in\mathbb{N}_0, n\in\mathbb{N}$ is odd and $b\in\mathcal{O}$ such that $N(b)$ is odd and $(1/m)b\notin\mathcal{O}$ for $m\in\mathbb{Z}$, $m>1$ (cf. [5], p. 37). Just as in [9] we define the *greatest invariant divisor* of a by

$$\mathrm{inv}(a):=(1+i)^en.$$

Given $a, b \in \mathcal{O} - \{0\}$ we say that a is a *total divisor* of b and write $a \| b$ if $a | \mathrm{inv}(b)$. Moreover a and b are called *similar* if $N(a) = N(b)$ and $\mathrm{inv}(a) = \mathrm{inv}(b)$ (cf. [9]).

An element $0 \neq a \in \mathcal{O}$ is said to be *completely primitive* if $\mathrm{inv}(a^m) = 1$ holds for all $m \in \mathbb{N}$. Given $m \in \mathbb{N}$ set

$$\mathcal{N}(m) := \{a \in \mathcal{O}; N(a) = m\}.$$

Properties of completely primitive elements are stated in

PROPOSITION 1

(a) *An element $0 \neq a \in \mathcal{O}$ is completely primitive if and only if* $\gcd(N(a), 2\,\mathrm{Re}(a)) = 1$.
(b) *Let p be an odd prime, then $\mathcal{N}(p)$ contains a completely primitive element.*

Proof

(a) Use the fact that $a^2 = 2\,\mathrm{Re}(a)a - N(a)$ holds for all $a \in \mathbb{H}$.
(b) Let $a \in \mathcal{N}(p)$. In view of part (a) it suffices to choose $\varepsilon \in \mathcal{E}$ satisfying

$$0 < \mathrm{Re}(a\varepsilon) < \tfrac{1}{2}p.$$

Then $a\varepsilon$ proves to be completely primitive. □

The application of the Hurwitz Decomposition Theorem in [5], Vorlesung 10, especially yields

PROPOSITION 2

Let p be an odd prime and $\pi \in \mathcal{N}(p)$ completely primitive. Given $m \in \mathbb{N}_0$ one has

$$\{a \in \mathcal{O}; a \| \pi^m\} = \{\varepsilon\pi^n; \varepsilon \in \mathcal{E}, 0 \leqslant n \leqslant m\},$$

$$\{a \in \mathcal{O}; a | \pi^m\} = \{\pi^n\varepsilon; \varepsilon \in \mathcal{E}, 0 \leqslant n \leqslant m\}.$$

As a slight modification of [9] we define for $a, b \in \mathcal{O}$ the torsion subgroup

$$\mathrm{Tor}(a, b) = \{c \in \mathcal{O}; ac \in \mathcal{O}b\}$$

of $\mathcal{O}$. In particular, one has for $\varepsilon \in \mathcal{E}$

$$\mathrm{Tor}(a, \varepsilon) = \mathcal{O}, \quad \mathrm{Tor}(\varepsilon, b) = \mathcal{O}b.$$

Let p be an odd prime and $\pi, \pi^* \in \mathcal{N}(p)$. Then [9], Lemma 2, yields

$$\#(\mathrm{Tor}(p, p)/\mathcal{O}p) = p^4, \quad \#(\mathrm{Tor}(\pi, p)/\mathcal{O}p) = p^2,$$

$$\#(\mathrm{Tor}(p, \pi^*)/\mathcal{O}\pi^*) = p^2, \quad \#(\mathrm{Tor}(\pi, \pi^*)/\mathcal{O}\pi^*) = p. \tag{3}$$

Let $l \in \mathbb{N}$ be odd. Then we need the isomorphism of the rings

$$\psi_l : \mathcal{O}/l\mathcal{O} \to \mathrm{Mat}(2; \mathbb{Z}/l\mathbb{Z})$$

given by A Hurwitz [5], Vorlesung 8. This isomorphism corresponds to the Peirce

decomposition of $\mathcal{O}/l\mathcal{O}$. Moreover ψ_l can be extended to an isomorphism

$$\psi_l : \mathrm{Mat}(n;\mathcal{O})/l\,\mathrm{Mat}(n;\mathcal{O}) \to \mathrm{Mat}(2n;\mathbb{Z}/l\mathbb{Z}). \tag{4}$$

$\mathcal{U}_n := GL(n;\mathcal{O})$ is defined to be the group of units in the ring $\mathrm{Mat}(n;\mathcal{O})$ and is called the *unimodular group of degree n*. Given $a = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$ set

$$\check{a} := \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix} \in \mathrm{Mat}(2;\mathbb{C}).$$

This map yields an embedding $^{\vee} : \mathrm{Mat}(n;\mathbb{H}) \to \mathrm{Mat}(2n;\mathbb{C})$ (cf. [7], p. 15). Then [7], I.2.6 and I.2.7, lead to

$$\det \check{A} \in \mathbb{N}_0 \quad \text{for } A \in \mathrm{Mat}(n;\mathcal{O}),$$

$$\mathcal{U}_n = \{U \in \mathrm{Mat}(n;\mathcal{O}); \det \check{U} = 1\}. \tag{5}$$

We are going to describe the Hecke-algebra in the case $\mathcal{S} := \mathcal{U}_n$ and

$$\mathcal{M} := \mathcal{M}_n := \mathcal{M}(n;\mathcal{O}) := \{A \in \mathrm{Mat}(n;\mathcal{O}); \det \check{A} \neq 0\}$$

$$= \mathrm{Mat}(n;\mathcal{O}) \cap GL(n;\mathbb{H}).$$

Moreover we need the determinantal subset

$$\mathcal{M}_n(q) := \{A \in \mathrm{Mat}(n;\mathcal{O}); \det \check{A} = q\}, \quad q \in \mathbb{N},$$

which decomposes into full double cosets modulo $\mathcal{U}_n$ in virtue of (5).

Lemma 1

(a) *Given $A \in \mathcal{M}_n$ the right coset $\mathcal{U}_n A$ possesses a representative $B = (b_{lm})$, which is a lower triangular matrix. B is uniquely determined, whenever the diagonal entries are chosen in a set of representatives of $\mathcal{O}\backslash\mathcal{O} - \{0\}$ and the off-diagonal entries b_{lm} in a set of representatives of $\mathcal{O}/\mathcal{O}b_{mm}$ for $1 \leqslant m < l \leqslant n$.*

(b) *Given $q \in \mathbb{N}$ then $\mathcal{M}_n(q)$ decomposes into finitely many right cosets modulo $\mathcal{U}_n$. Especially $(\mathcal{U}_n, \mathcal{M}_n)$ satisfies the Hecke-condition* (1).

Proof

(a) Apply [7], I.2.5. Then proceed in the same way as in [12], Theorems II.2 and II.3.

(b) Observe that $\#\{a \in \mathcal{O}; N(a) \leqslant q\} < \infty$. In view of $\det B = N(b_{11}) \cdot \ldots \cdot N(b_{nn})$ there are only finitely many possibilities for the diagonal entries of B. Given $0 \neq b \in \mathcal{O}$ then $\#(\mathcal{O}/\mathcal{O}b) = N(b)^2$ holds in virtue of [9], Proposition 4. □

2.3. *The decomposition into primary components*

Consider the Hecke-algebra $\mathcal{H}_n := \mathcal{H}(\mathcal{U}_n, \mathcal{M}_n)$.

PROPOSITION 3

Given $A, B \in \mathcal{M}_n$, then

$$(\mathcal{U}_n A \mathcal{U}_n) \cdot (\mathcal{U}_n B \mathcal{U}_n) = \mathcal{U}_n A B \mathcal{U}_n$$

holds, whenever one of the following conditions is fulfilled:

(i) $A = cU$ *or* $B = cU$, *where* $c \in \mathrm{Inv}\,\mathcal{O}$ *and* $U \in \mathcal{U}_n$.
(ii) *One has* $n \geqslant 2$, $A \in \mathcal{M}_n(l)$ *and* $B \in \mathcal{M}_n(m)$, *where* $l, m \in \mathbb{N}$ *are relatively prime.*

Proof

(i) The statement follows from the definition (2) of the product in view of $\mathcal{U}_n(cU) = (cU)\mathcal{U}_n$.
(ii) At first [9], Theorems 3 and 4, yield $\mathcal{U}_n A \mathcal{U}_n B \mathcal{U}_n = \mathcal{U}_n A B \mathcal{U}_n$.

Thus

$$(\mathcal{U}_n A \mathcal{U}_n)\cdot(\mathcal{U}_n B \mathcal{U}_n) = t \mathcal{U}_n A B \mathcal{U}_n \quad \text{for some } t \in \mathbb{N}$$

follows. In order to prove $t = 1$, choose disjoint coset decompositions

$$\mathcal{U}_n A \mathcal{U}_n = \bigcup_p \mathcal{U}_n A_p, \quad \mathcal{U}_n B \mathcal{U}_n = \bigcup_q \mathcal{U}_n B_q.$$

It suffices to show that the right cosets $\mathcal{U}_n A_p B_q$ are mutually distinct. Let $U \in \mathcal{U}_n$ be given such that $U A_p B_q = A_r B_s$, i.e.

$$A_r^{-1} U A_p = B_s B_q^{-1}. \tag{*}$$

Now observe that $l(A_r^{-1} U A_p) \in \mathrm{Mat}(n; \mathcal{O})$ and $m(B_s B_q^{-1}) \in \mathrm{Mat}(n; \mathcal{O})$. Since l, m are relatively prime, both sides of (*) are integral. Then $\det B_s = \det B_q = m$ and (5) imply $B_s B_q^{-1} \in \mathcal{U}_n$, hence $B_s = B_q$. Finally $U A_p = A_r$ leads to $A_p = A_r$. □

In order to describe $\mathcal{H}_n$, we need the submonoid

$$\mathcal{M}_{n,p} := \bigcup_{l=0}^{\infty} \mathcal{M}_n(p^l)$$

for a prime p and the subalgebra $\mathcal{H}_{n,p} := \mathcal{H}(\mathcal{U}_n, \mathcal{M}_{n,p})$ of $\mathcal{H}_n$. We call $\mathcal{H}_{n,p}$ the *p-primary component* of $\mathcal{H}_n$.

Theorem 2. *If* $n \geqslant 2$, *then* $\mathcal{H}_n$ *is commutative and coincides with the tensor product of its primary components, i.e.*

$$\mathcal{H}_n = \bigotimes_p \mathcal{H}_{n,p},$$

where p runs through all prime numbers in $\mathbb{N}$.

Proof. Let $A \in \mathcal{M}_n$, then the double coset $\mathcal{U}_n A \mathcal{U}_n$ possesses a representative in elementary divisor form. Now [9], Theorems 1, 2 and 4, imply

$$\mathcal{U}_n A \mathcal{U}_n = \mathcal{U}_n \bar{A}' \mathcal{U}_n.$$

The commutativity of $\mathcal{H}_n$ follows from [14], Proposition 3.8.

It is clear from the elementary divisor theory and [7], I.1.13, that each $A \in \mathcal{M}_n$ can be written as a product of matrices, where each factor belongs to some $\mathcal{M}_{n,p}$. Now Proposition 3 completes the proof, since the double cosets $\mathcal{U}_n A \mathcal{U}_n$, $A \in \mathcal{M}_n$, form a basis of $\mathcal{H}_n$. □

The case $n=1$ was excluded, since it becomes exceptional.

Lemma 2. The Hecke-algebra $\mathscr{H}_1$ is not commutative. More precisely the centre of $\mathscr{H}_1$ equals $\mathscr{H}(\mathscr{E},\mathscr{E}\mathbb{N})$ and is isomorphic to the semigroup algebra $\mathbb{Z}[\mathbb{N}]$ of $\mathbb{N}$ over $\mathbb{Z}$.

Proof. Clearly the subalgebra $\mathscr{H}(\mathscr{E},\mathscr{E}\mathbb{N})$ is contained in the centre of $\mathscr{H}_1$, since the centre of $\mathcal{O}$ equals $\mathbb{Z}$. On the other hand suppose that

$$T=\sum_{l=1}^{m} t_l \mathscr{E} a_l \mathscr{E}, \quad 0\neq t_l\in\mathbb{Z}, \quad 0\neq a_l\in\mathcal{O},$$

belongs to the centre of $\mathscr{H}_1$. Then it especially follows that for $1\leqslant l\leqslant m$ and $0\neq b\in\mathcal{O}$ there exist $q, 1\leqslant q\leqslant m$, and $\varepsilon_1,\varepsilon_2,\varepsilon_3\in\mathscr{E}$ satisfying $a_l b=\varepsilon_1 b\varepsilon_2 a_q\varepsilon_3$. Now use the isomorphism (4) for $n=1$ and a sufficiently large prime p. Hence we have $A_1,\ldots,A_m$ in $\mathrm{Mat}(2;\mathbb{Z}/p\mathbb{Z})$ and 24 possibilities for $U_1,U_2,U_3\in GL(2;\mathbb{Z}/p\mathbb{Z})$ such that the equation

$$A_l B=U_1 B U_2 A_q U_3 \qquad (*)$$

has a solution for $1\leqslant l\leqslant m$ and all $B\in\mathrm{Mat}(2;\mathbb{Z}/p\mathbb{Z})$. If A_l, A_q, U_1, U_2, U_3 are fixed, the equation (*) has only p^3 solutions B, except for $A_l=tU_1$ and $U_2A_qU_3=tI$ for some $t\in\mathbb{Z}/p\mathbb{Z}$. If p is large enough, $T\in\mathscr{H}(\mathscr{E},\mathbb{N}\mathscr{E})$ follows. □

2.4. *Right coset decompositions*

According to Theorem 2 we may restrict ourselves to the investigation of the primary components. Therefore it is necessary to describe the right coset decompositions for all the double cosets $\mathscr{U}_n A\mathscr{U}_n$, where $A\in\mathscr{M}_n$ such that $pA^{-1}\in\mathrm{Mat}(n;\mathcal{O})$.

We start with the (simpler) case $p=2$. Note that $\mathbb{F}:=\mathcal{O}/(1+i)\mathcal{O}$ is a field with 4 elements. If $A\in\mathrm{Mat}(n;\mathcal{O})$, then $r_2(A)$ denotes the rank of A over $\mathbb{F}$. Clearly one has

$$r_2(UAV)=r_2(A) \quad \text{for } U,V\in\mathscr{U}_n.$$

According to the elementary divisor theory (cf. [9] or [17]) each double coset $\mathscr{U}_n A\mathscr{U}_n$, $A\in\mathscr{M}_{n,2}$, possesses a unique representative

$$A=[(1+i)^{l_1},\ldots,(1+i)^{l_n}], \quad 0\leqslant l_1\leqslant\cdots\leqslant l_n.$$

We define the double cosets

$$T_l^{(n)}(1+i):=\mathscr{U}_n[I^{(n-l)},(1+i)I^{(l)}]\mathscr{U}_n, \quad l=0,1,\ldots,n,$$

in $\mathscr{H}_{n,2}$. Given $A\in\mathrm{Mat}(n;\mathcal{O})$ one has the obvious criterion

$$A\in T_l^{(n)}(1+i)\Leftrightarrow r_2(A)=n-l \quad \text{and} \quad \det\check{A}=2^l.$$

If $X_1,\ldots,X_n$ are indeterminates and $0\leqslant l\leqslant n$, let

$$E_l^{(n)}(X_1,\ldots,X_n):=\sum_{\substack{(\varepsilon_1,\ldots,\varepsilon_n)\in\{0,1\}^n\\ \varepsilon_1+\cdots+\varepsilon_n=l}} X_1^{\varepsilon_1}\cdot\ldots\cdot X_n^{\varepsilon_n}$$

denote the *l-th elementary symmetric polynomial* in $X_1,\ldots,X_n$.

Now we can apply the same arguments, which were used in the proof of [3], IV.2.7, in order to obtain

Lemma 3. If $0 \leqslant l \leqslant n$ a set of representatives of $\mathscr{U}_n \backslash T_l^{(n)}(1+i)$ is given by the integral matrices

$$A = \begin{pmatrix} (1+i)^{m_1} & & 0 \\ & \ddots & \\ a_{\mu\nu} & & (1+i)^{m_n} \end{pmatrix},$$

which satisfy

(i) $m_\nu \in \{0, 1\}$ *for* $1 \leqslant \nu \leqslant n$,
(ii) $m_1 + \cdots + m_n = l$,
(iii) $a_{\mu\nu}$ *runs through a set of representatives of* $\mathfrak{O}/(1+i)^{m_\nu}\mathfrak{O}$ *for* $1 \leqslant \nu < \mu \leqslant n$,
(iv) $a_{\mu\nu} = 0$, *if* $m_\nu = m_\mu = 1$.

Especially one has

$$\deg T_l^{(n)}(1+i) = 2^{-l(l+1)} E_l^{(n)}(2^2, 2^4, \ldots, 2^{2n}).$$

Now we consider an odd prime p. Given $A \in \mathrm{Mat}(n; \mathfrak{O})$ we use the isomorphism (4) in order to define $r_p(A) := \operatorname{rank} \psi_p(A + p\,\mathrm{Mat}(n; \mathfrak{O}))$. Hence one has $0 \leqslant r_p(A) \leqslant 2n$ and

$$r_p(UAV) = r_p(A) \quad \text{for } U, V \in \mathscr{U}_n.$$

According to Proposition 1 we choose a completely primitive $\pi \in \mathscr{N}(p)$. If $n \geqslant 2$, then [9] yields that each double coset $\mathscr{U}_n A \mathscr{U}_n$, $A \in \mathscr{M}_{n,p}$, possesses a unique representative

$$A = [\pi^{l_1} p^{m_1}, \ldots, \pi^{l_n} p^{m_n}], \quad 0 \leqslant l_\nu, \quad 0 \leqslant m_\nu, \quad l_\nu + m_\nu \leqslant m_{\nu+1} \quad \text{for all } \nu. \tag{6}$$

Whenever $n \geqslant 2$ we define the double cosets

$$R_{2l}^{(n)}(p) = \mathscr{U}_n [I^{(n-l)}, pI^{(l)}] \mathscr{U}_n, \quad 0 \leqslant l \leqslant n,$$

$$R_{2l-1}^{(n)}(p) = \mathscr{U}_n [I^{(n-l)}, \pi, pI^{(l-1)}] \mathscr{U}_n, \quad 1 \leqslant l \leqslant n.$$

Given $A \in \mathscr{M}_n$ we again have the simple but effective criterion

$$A \in R_l^{(n)}(p) \Leftrightarrow r_p(A) = 2n - l \quad \text{and} \quad \det \check{A} = p^l. \tag{7}$$

The analogue of Lemma 3 is more complicated. Especially it is more convenient to choose products of matrices.

Lemma 4. Let p be an odd prime, $n \geqslant 2$ and $0 \leqslant l \leqslant 2n$. Then a set of representatives of $\mathscr{U}_n \backslash R_l^{(n)}(p)$ is given by the products of the following integral matrices

$$\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ b_{\mu\nu} & & 1 \end{pmatrix}, \quad N(a_\nu) = p^{m_\nu}, \quad 1 \leqslant \nu \leqslant n,$$

which satisfy

(i) $a_\nu = 1$ *or* $a_\nu = p$ *or* a_ν *runs through a set of representatives of* $\mathscr{E} \backslash \mathscr{N}(p)$ *for* $1 \leqslant \nu \leqslant n$,

(ii) $m_1 + \cdots + m_n = l$,
(iii) $b_{\mu\nu}$ *runs through a set of representatives of* $\mathcal{O}/\mathrm{Tor}(a_\mu, a_\nu)$ *for* $1 \leqslant \nu < \mu \leqslant n$.

Especially one has

$$\deg R_l^{(n)}(p) = p^{-l(l+1)/2} E_l^{(2n)}(p, p^2, \ldots, p^{2n}).$$

Proof. Clearly the matrices above belong to $R_l^{(n)}(p)$ in view of (7). The attached right cosets are mutually distinct in virtue of (i), (iii) and Lemma 1.

Now consider a right coset $\mathcal{U}_n A \subset R_l^{(n)}(p)$ and choose a representative

$$A = (a_{\mu\nu}), \quad a_\nu = a_{\nu\nu}, \quad a_{\mu\nu} = 0 \quad \text{for } \mu < \nu,$$

in the form of Lemma 1. At first $pA^{-1} \in \mathrm{Mat}(n; \mathcal{O})$ yields $pa_\nu^{-1} \in \mathcal{O}$, hence (i). Using (7) we get (ii) in view of

$$N(a_1) \cdot \cdots \cdot N(a_n) = \det \breve{A} = p^l.$$

Moreover (7) yields

$$r_p(A) = r_p([a_1, \ldots, a_n]) = 2n - l.$$

This condition leads to

$$r_p\left(\begin{pmatrix} a_\nu & 0 \\ a_{\mu\nu} & a_\mu \end{pmatrix}\right) = r_p\left(\begin{pmatrix} a_\nu & 0 \\ 0 & a_\mu \end{pmatrix}\right) \quad \text{for } 1 \leqslant \nu < \mu \leqslant n.$$

Considering the special possibilities for the diagonal entries according to (i), we conclude that there exists $a \in \mathcal{O}$ satisfying $a_{\mu\nu} + aa_\nu \in a_\mu \mathcal{O}$. Moreover we can choose a in an appropriate way such that $b_{\mu\nu} := a_\mu^{-1}(a_{\mu\nu} + aa_\nu)$ belongs to the fixed set of representatives of $\mathcal{O}/\mathrm{Tor}(a_\mu, a_\nu)$. Fulfilling these conditions successively for $1 \leqslant \nu < \mu \leqslant n$, we obtain a set of representatives in the desired form.

Set $N(a_\nu) = p^{m_\nu}$ for $1 \leqslant \nu \leqslant n$. If $1 \leqslant \nu < \mu \leqslant n$, we can apply (3) in order to calculate

$$\#(\mathcal{O}/\mathrm{Tor}(a_\mu, a_\nu)) = \frac{\#(\mathcal{O}/\mathcal{O}a_\nu)}{\#(\mathrm{Tor}(a_\mu, a_\nu)/\mathcal{O}a_\nu)} = p^{2m_\nu - m_\nu m_\mu}.$$

If $a_1, \ldots, a_m$ are fixed the number of these matrices therefore equals

$$\prod_{1 \leqslant \nu < \mu \leqslant n} p^{m_\nu(2 - m_\mu)}.$$

Now $\#(\mathcal{O}^\times \backslash \mathcal{N}(p)) = p + 1$ holds due to [5], Vorlesung 9. Thus we calculate

$$\begin{aligned} &\deg R_l^{(n)}(p) \\ &= \sum_{\substack{(m_1, \ldots, m_n) \in \{0,1,2\}^n \\ m_1 + \cdots + m_n = l}} \left(\prod_{\sigma=1}^{n} (p+1)^{m_\sigma(2 - m_\sigma)} \right) \left(\prod_{1 \leqslant \nu < \mu \leqslant n} p^{m_\nu(2 - m_\mu)} \right) \\ &= p^{\frac{1}{2}l(l+1)} E_l^{(2n)}(p, p^2, \ldots, p^{2n}), \end{aligned}$$

where the last equality can be proved by induction on n. □

2.5. *The primary components*

We now describe the structure of the primary components of the Hecke-algebra $\mathscr{H}_n$. Observe that $\mathscr{H}_{n,p}$ becomes a $\mathbb{Z}$-graded algebra, i.e.

$$\mathscr{H}_{n,p} = \bigoplus_{q=0}^{\infty} \mathscr{H}_{n,p}^{(q)},$$

where

$$\mathscr{H}_{n,p}^{(q)} = \mathscr{H}(\mathscr{U}_n, \mathscr{M}_n(p^q)).$$

Theorem 3

(a) *$\mathscr{H}_{n,2}$ equals the polynomial ring over $\mathbb{Z}$ in n elements*

$$T_1^{(n)}(1+i), \ldots, T_n^{(n)}(1+i),$$

which are algebraically independent.

(b) *Let $n \geqslant 2$ and p be an odd prime. Then $\mathscr{H}_{n,p}$ equals the polynomial ring over $\mathbb{Z}$ in $2n$ elements*

$$R_1^{(n)}(p), \ldots, R_{2n}^{(n)}(p),$$

which are algebraically independent. Especially $\mathscr{H}_n$ does not contain any zero-divisors.

Proof

(a) Proceed in the same way as in the more complicated proof of part (b) or follow G Shimura [14], Chapter 3.2.

(b) Set $\mathscr{A} = \mathbb{Z}[R_1^{(n)}(p), \ldots, R_{2n}^{(n)}(p)] \subset \mathscr{H}_{n,p}$. We show by induction on q that $\mathscr{H}_{n,p}^{(q)} \subset \mathscr{A}$ holds. Here the cases $q = 0, 1$ are trivial in view of $\mathscr{H}_{n,p}^{(0)} = \mathbb{Z}\mathscr{U}_n$ and $\mathscr{H}_{n,p}^{(1)} = \mathbb{Z}R_1^{(n)}(p)$. Given $q \geqslant 2$ we show successively that the submodule

$$\mathscr{H}_{n,p}^{(q,r)} = \left\{ \sum_{\substack{A:\mathscr{U}_n\backslash\mathscr{U}_nA\mathscr{U}_n\mathscr{U}_n/\mathscr{U}_n \\ \nu_p(A)=r}} t(\mathscr{U}_nA\mathscr{U}_n)\mathscr{U}_nA\mathscr{U}_n;\ t(\mathscr{U}_nA\mathscr{U}_n) \in \mathbb{Z} \right\}$$

is contained in $\mathscr{A}$. Given a double coset $\mathscr{U}_nA\mathscr{U}_n \in \mathscr{H}_{n,p}^{(q,r)}$ choose the representative A in the form (6), where

$$O = l_1 = \cdots = l_s = m_1 = \cdots = m_s \quad \text{and} \quad m_{s+1} > 0, \quad \text{if } r = 2s, \quad 0 \leqslant s \leqslant n,$$

$$O = l_1 = \cdots = l_{s-1} = m_1 = \cdots = m_s \quad \text{and} \quad l_s > 0, \quad \text{if } r = 2s-1, \quad 1 \leqslant s \leqslant n.$$

If $r = 0$ one has $B = (pI)^{-1}A \in \mathrm{Mat}(n; \mathscr{O})$. The induction hypothesis and Proposition 3 yield

$$\mathscr{U}_nA\mathscr{U}_n = R_{2n}^{(n)}(p) \cdot (\mathscr{U}_nB\mathscr{U}_n) \in \mathscr{A}.$$

The case $r = 2n$ coincides with $\mathscr{U}_nA\mathscr{U}_n = \mathscr{U}_n$. Hence let $0 < r < 2n$ and consider

$$B = [1, \ldots, 1, \pi^{l_{s+1}} p^{m_{s+1}-1}, \ldots, \pi^{l_n} p^{m_n-1}], \quad \text{if } r = 2s,$$

$$B = [1, \ldots, 1, \pi^{l_s-1}, \pi^{l_{s+1}} p^{m_{s+1}-1}, \ldots, \pi^{l_n} p^{m_n-1}], \quad \text{if } r = 2s-1.$$

The hypothesis yields $\mathcal{U}_n B \mathcal{U}_n \in \mathcal{A}$. Now we compute

$$(\mathcal{U}_n B \mathcal{U}_n) \cdot R_{2n-r}^{(n)}(p) = \sum_{C: \mathcal{U}_n \backslash \mathcal{M}_n(p^q)/\mathcal{U}_n} t(\mathcal{U}_n C \mathcal{U}_n) \mathcal{U}_n C \mathcal{U}_n.$$

At first $t(\mathcal{U}_n C \mathcal{U}_n) \neq 0$ implies $r_p(C) \leqslant r$ in view of (7). Consider $C \in \mathcal{M}_n(p^q)$ with $r_p(C) = r$ in the form (6), i.e.

$$C = [1, \ldots, 1, \pi^{\nu_{s+1}} p^{\mu_{s+1}}, \ldots, \pi^{\nu_n} p^{\mu_n}], \quad \mu_{s+1} > 0, \quad \text{if } r = 2s,$$

$$C = [1, \ldots, 1, \pi^{\nu_s}, \pi^{\nu_{s+1}} p^{\mu_{s+1}}, \ldots, \pi^{\nu_n} p^{\mu_n}], \quad \nu_s > 0, \quad \text{if } r = 2s - 1.$$

Choose the representatives G of $\mathcal{U}_n \backslash R_{2n-r}^{(n)}(p)$ according to Lemma 4 and B^* of $\mathcal{U}_n \backslash \mathcal{U}_n B \mathcal{U}_n$ in the form of Lemma 1 such that

$$B^* G = UC \quad \text{for some } U \in \mathcal{U}_n.$$

The choice of C and Lemma 4 yield

$$G = [I^{(s)}, pI^{(n-s)}], \quad \text{if } r = 2s,$$

$$G = [I^{(s-1)}, a, pI^{(n-s)}], \quad \text{if } r = 2s - 1, \quad \text{where } a \in \mathcal{N}(p).$$

In view of $a|_r \pi^{\nu_s}$ Proposition 2 implies $\mathcal{E}a = \mathcal{E}\pi$, hence $a = \pi$. Thus the right coset $\mathcal{U}_n B^*$ is uniquely determined and Lemma 1 yields $B^* = CG^{-1}$. Now B^* has the form (6) and $t(\mathcal{U}_n C \mathcal{U}_n) = 1$ holds for $\mathcal{U}_n C \mathcal{U}_n = \mathcal{U}_n B \mathcal{U}_n$ as well as $t(\mathcal{U}_n C \mathcal{U}_n) = 0$ otherwise. Thus we have

$$(\mathcal{U}_n B \mathcal{U}_n) \cdot R_{2n-r}^{(n)}(p) = T + \mathcal{U}_n A \mathcal{U}_n,$$

where

$$T \in \bigoplus_{l=0}^{r-1} \mathcal{H}_{n,p}^{(q,l)}.$$

The hypothesis yields $\mathcal{U}_n A \mathcal{U}_n \in \mathcal{A}$, hence $\mathcal{A} = \mathcal{H}_{n,p}$.

In view of (6) we calculate

$$\begin{aligned} \dim \mathcal{H}_{n,p}^{(q)} &= \#\{(l_1, m_1, \ldots, l_n, m_n)' \in \mathbb{N}_0^{2n}; l_\nu + m_\nu \leqslant m_{\nu+1}, \\ &\qquad l_1 + 2m_1 + \cdots + l_n + 2m_n = q\} \\ &= \#\{(q_1, \ldots, q_{2n})' \in \mathbb{N}_0^{2n}; q_1 \leqslant \cdots \leqslant q_{2n}, q_1 + \cdots + q_{2n} = q\} \\ &= p_{2n}(q), \end{aligned}$$

where $p_{2n}(q)$ denotes the number of partitions of q into at most $2n$ parts. Since $\mathcal{H}_{n,p}$ is a $\mathbb{Z}$-graded algebra, the monomial

$$R_1^{(n)}(p)^{q_1} \cdot \ldots \cdot R_{2n}^{(n)}(p)^{q_{2n}}, \quad q_\nu \in \mathbb{N}_0,$$

belongs to $\mathcal{H}_{n,p}^{(q)}$ if and only if

$$\sum_{\nu=1}^{2n} \nu q_\nu = q.$$

In view of [1], Theorem 14.1, the number of these monomials also equals $p_{2n}(q)$. Since $R_1^{(n)}(p), \ldots, R_{2n}^{(n)}(p)$ generate $\mathscr{H}_{n,p}$, they prove to be algebraically independent. □

Remark 1.

(a) The proof in [14] resp. [3] proceeds in a different way. In these papers a homomorphism between $\mathscr{H}_n$ and $\mathscr{H}_{n-1}$ is used. Given $n \geqslant 3$ and a matrix $A = [a_1, \ldots, a_n] \in \mathscr{M}_n$ satisfying $a_1 \| a_2 \| \cdots \| a_n$, define

$$\phi(\mathscr{U}_n A \mathscr{U}_n) = \begin{cases} \mathscr{U}_{n-1}[a_2, \ldots, a_n]\mathscr{U}_{n-1} & \text{if } a_1 \in \mathscr{E} \\ 0 & \text{otherwise} \end{cases}.$$

By linear extension we obtain a map $\phi: \mathscr{H}_n \to \mathscr{H}_{n-1}$, which turns out to be a surjective homomorphism of the $\mathbb{Z}$-algebras. According to Theorem 3 the kernel of the restriction of ϕ to $\mathscr{H}_{n,p}$ is an ideal in $\mathscr{H}_{n,p}$, which is generated by

$$\begin{aligned} &T_n^{(n)}(1+i), && \text{if } p = 2, \\ &R_{2n}^{(n)}(p) \quad \text{and} \quad R_{2n-1}^{(n)}(p), && \text{if } p \text{ is an odd prime.} \end{aligned}$$

(b) It is also possible to define a commutative subalgebra of $\mathscr{H}_1$, which has the corresponding structure to $\mathscr{H}_n, n \geqslant 2$.
This subalgebra is generated by the centre of $\mathscr{H}_1$ and the elements

$$T_1(l) := \sum_{a: \mathscr{E} \backslash \mathscr{E} l \mathscr{E} / \mathscr{E}} \mathscr{E} a \mathscr{E}, \quad l \in \mathbb{N}.$$

Therefore one has to observe that

$$T_1(l) \cdot T_1(m) = T_1(lm),$$

whenever $l, m \in \mathbb{N}$ are relatively prime,

$$T_1(2^l) = T_1(2)^l \quad \text{for } l \in \mathbb{N}_0,$$

$$T_1(p^r) \cdot T_1(p^s) = \sum_{\nu=0}^{\min(r,s)} p^\nu (\mathscr{E} p \mathscr{E})^\nu T_1(p^{r+s-2\nu})$$

for $r, s \in \mathbb{N}_0$, whenever p is an odd prime. These identities can easily be proved by the Hurwitz Decomposition Theorem in [5], Vorlesung 10. For an odd prime p they correspond to the products in the Hecke-algebra related to $GL(2; \mathbb{Z})$.

2.6. *A formal power series*

At first we compute the product of the generating double cosets with certain linear combinations given by determinantal conditions. For $l \in \mathbb{N}$ set

$$T_n(l) := \sum_{A: \mathscr{U}_n \backslash \mathscr{M}_n(l) / \mathscr{U}_n} \mathscr{U}_n A \mathscr{U}_n \in \mathscr{H}_n.$$

Lemma 5

(a) *Let $0 \leqslant l \leqslant n$ and $q \in \mathbb{N}$. Then one has*

$$T_l^{(n)}(1+i)\cdot T_n(2^q)$$

$$= \sum_{m=l}^{n} 2^{-l(l+1)} E_l^{(m)}(2^2,\ldots,2^{2m}) \sum_{\substack{A:\mathscr{U}_n\backslash\mathscr{U}_n\begin{pmatrix}2^{q+l}\\ & 1\end{pmatrix}\mathscr{U}_n \\ r_2(A)=n-m}} \mathscr{U}_n A \mathscr{U}_n.$$

(b) *Let p be an odd prime, $q\in\mathbb{N}$, $n\geqslant 2$ and $0\leqslant l\leqslant 2n$. Then one has*

$$R_l^{(n)}(p)\cdot T_n(p^q)$$

$$= \sum_{m=l}^{2n} p^{-l(l+1)/2} E_l^{(m)}(p,\ldots,p^m) \sum_{\substack{A:\mathscr{U}_n\backslash\mathscr{U}_n\begin{pmatrix}p^{q+l}\\ & 1\end{pmatrix}\mathscr{U}_n \\ r_p(A)=2n-m}} \mathscr{U}_n A \mathscr{U}_n.$$

Proof

(a) Proceed in the same way as in part (b) or follow G Shimura [14], Lemma 3.22.
(b) Set

$$T_n(p^q)\cdot R_l^{(n)}(p) = \sum_{A:\mathscr{U}_n\backslash\mathscr{U}_n\begin{pmatrix}p^{q+l}\\ & 1\end{pmatrix}\mathscr{U}_n} t(\mathscr{U}_n A\mathscr{U}_n)\mathscr{U}_n A\mathscr{U}_n.$$

Clearly $t(\mathscr{U}_n A\mathscr{U}_n)\neq 0$ implies $r_p(A)\leqslant 2n-l$ in view of (7). Let $l\leqslant m\leqslant 2n$ and assume $r_p(A)=2n-m$. We choose A in the form (6)

$$A=[1,\ldots,1,\pi^{\nu_{s+1}}p^{\mu_{s+1}},\ldots,\pi^{\nu_n}p^{\mu_n}],\quad \mu_{s+1}>0,\quad \text{if } 2n-m=2s,$$

$$A=[1,\ldots,1,\pi^{\nu_s},\pi^{\nu_{s+1}}p^{\mu_{s+1}},\ldots,\pi^{\nu_n}p^{\mu_n}],\quad \nu_s>0,\quad \text{if } 2n-m=2s-1.$$

Consider the representatives G of $\mathscr{U}_n\backslash R_l^{(n)}(p)$ according to Lemma 4 and B of $\mathscr{U}_n\backslash\mathscr{M}_n(p^q)$ due to Lemma 1 such that

$$BG=UA \quad \text{for some } U\in\mathscr{U}_n.$$

At first let $2n-m=2s$, then the choice of A and Lemma 4 yield

$$G=[I^{(s)},H],$$

where H runs through a set of representatives of $\mathscr{U}_{m/2}\backslash R_l^{m/2}(p)$. In virtue of $1\leqslant\mu_{s+1}\leqslant\cdots\leqslant\mu_n$ we conclude

$$AG^{-1}\in\mathrm{Mat}(n;\mathscr{O})$$

for all these matrices H. Thus

$$t(\mathscr{U}_n A\mathscr{U}_n)=\deg R_l^{m/2}(p)=p^{-l(l+1)/2}E_l^{(m)}(p,\ldots,p^m)$$

follows, whenever $r_p(A)=2n-m$ is even.

Next let $2n-m=2s-1$ be odd. Then the choice of A, Proposition 2 and Lemma 4 yield

$$G=[I^{(s)},H],$$

$$G = \begin{pmatrix} I & 0 & 0 \\ 0 & \pi & 0 \\ 0 & g & H \end{pmatrix}, \quad I = I^{(s-1)},$$

where H runs through a set of representatives of $\mathscr{U}_{n-s}\backslash R_{l-1}^{(n-s)}(p)$ and for each H there are $p^{2(n-s)-(l-1)}$ possibilities for the integral vector $g \in \mathscr{O}^{n-s}$. Again we obtain

$$AG^{-1} \in \mathrm{Mat}(n; \mathscr{O})$$

for each of these choices of G. Thus Lemma 4 leads to

$$\begin{aligned} t(\mathscr{U}_n A \mathscr{U}_n) &= \deg R_l^{(n-s)}(p) + p^{2n+1-2s-l} \deg R_{l-1}^{(n-s)}(p) \\ &= p^{-l(l+1)/2} E_l^{(m)}(p, \ldots, p^m). \end{aligned}$$

□

Furthermore we need

PROPOSITION 4

Given $n \in \mathbb{N}$ and an indeterminate X, one has

$$\sum_{l=0}^{n} (-1)^l X^{-l} E_l^{(n)}(X, \ldots, X^n) = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{if } n > 0. \end{cases}$$

Proof. Given $n \geqslant 1$ one easily checks

$$\begin{aligned} &\sum_{l=0}^{n} (-1)^l X^{-l} E_l^{(n)}(X, \ldots, X^n) \\ &= (1 - X^{n-1}) \sum_{l=0}^{n-1} (-1)^l X^{-l} E_l^{(n-1)}(X, \ldots, X^{n-1}). \end{aligned}$$

□

In analogy with [14], Theorem 3.21, we obtain

Theorem 4

(a) $$\sum_{m=0}^{\infty} T_n(2^m) X^m = \left(\sum_{l=0}^{n} (-1)^l 2^{l(l-1)} T_l^{(n)}(1+i) X^l \right)^{-1}$$

holds formally in X.

(b) *Let $n \geqslant 2$ and p be an odd prime. Then*

$$\sum_{m=0}^{\infty} T_n(p^m) X^m = \left(\sum_{l=0}^{2n} (-1)^l p^{l(l-1)/2} R_l^{(n)}(p) X^l \right)^{-1}$$

holds formally in X.

Proof. We only deal with part (b), because (a) is proved in the same way. The use of Lemma 5 yields

$$\left(\sum_{l=0}^{2n} (-1)^l p^{l(l-1)/2} R_l^{(n)}(p) X^l \right) \left(\sum_{q=0}^{\infty} T_n(p^q) X^q \right)$$

$$= \sum_{l=0}^{2n} (-1)^l p^{-l} \sum_{m=l}^{2n} E_l^{(m)}(p, \ldots, p^m) \sum_{q=0}^{\infty} \sum_{\substack{B: \mathcal{U}_n \supset B \supset \mathcal{U}_n(p^{q+1}) \\ r_p(B) = 2n-m}} (\mathcal{U}_n B \mathcal{U}_n) X^{q+1}.$$

Due to Proposition 4 all the terms but $m = l = 0$ vanish, and the remaining term equals 1. □

Proposition 3 immediately yields

$$T_n(l) \cdot T_n(m) = T_n(lm),$$

whenever $l, m \in \mathbb{N}$ are relatively prime. Thus Theorem 4 implies

COROLLARY 1

If $n \geqslant 2$ *then*

$$\sum_{m=1}^{\infty} T_n(m) m^{-s} = \left(\sum_{l=0}^{n} (-1)^l T_l^{(n)} (1+i) 2^{l(l-1)-ls} \right)^{-1}$$

$$\times \prod_{\substack{p \text{ odd} \\ \text{prime}}} \left(\sum_{l=0}^{2n} (-1)^l R_l^{(n)}(p) p^{(1/2)l(l-1)-ls} \right)^{-1}$$

holds formally in s.

Finally we consider the simplest representation

$$\mathcal{H}_n \to \mathbb{Z}, \quad T \mapsto \deg T.$$

Therefore we need the zeta function attached to $\mathcal{O}$, i.e.

$$\zeta_{\mathcal{O}}(s) := \sum_{a: \mathcal{O} - \{0\}} N(a)^{-s} = \tfrac{1}{24} \sum_{0 \neq a \in \mathcal{O}} N(a)^{-s},$$

which converges absolutely for all complex s with $\mathrm{Re}(s) > 2$. We can apply the Hurwitz Decomposition Theorem [5], Vorlesung 10, or quote [19], p. 64, in a more general context in order to obtain

$$\zeta_{\mathcal{O}}(s) = (1 - 2^{1-s}) \zeta(s) \zeta(s-1),$$

where ζ denotes the Riemann zeta function. Using Lemma 1 we get

$$\sum_{m=1}^{\infty} \deg T_n(m) m^{-s} = \prod_{l=0}^{n-1} \zeta_{\mathcal{O}}(s-2l)$$

for $n \geqslant 1$ and all complex s with $\mathrm{Re}(s) > 2n$.

3. The Hecke-algebra related to the modular group

In this paragraph we investigate the structure of the Hecke-algebra related to the modular group of quaternions (cf. [7]).

Siegel modular group, but also related to those Hermitian modular groups, which can be treated in the same way. Therefore let $o = \mathbb{Z}$ or let o be the ring of integers in an imaginary quadratic number field of class number one. Hence o proves to be a principal ideal domain and we can apply the results of § 2.1.

Let $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in \mathrm{Mat}(2n; \mathbb{R})$. Given $l \in \mathbb{N}$ and a prime p set

$$\Delta_n(l) := \Delta_n^o(l) := \{M \in \mathrm{Mat}(2n; o);\ \bar{M}' J M = lJ\},$$

$$\Delta_n = \Delta_n^o := \bigcup_{l=1}^{\infty} \Delta_n^o(l), \quad \Delta_{n,p} = \Delta_{n,p}^o = \bigcup_{l=0}^{\infty} \Delta_n^o(p^l).$$

Especially $\Gamma_n := \Gamma_n^o := \Delta_n^o(1)$ is a group. $\Gamma_n^{\mathbb{Z}}$ is called the *Siegel modular group of degree n* and was investigated by C L Siegel [15]. In the case of an imaginary quadratic number field Γ_n^o is called the *Hermitian modular group of degree n associated with* o. The corresponding theory of Hermitian modular forms was developed by H Braun [2]. The Hecke-algebra and Hecke-operators related to the Siegel modular group were already applied by H Maaß [11], whereas the Hecke-algebra related to $\Gamma_2^{\mathbb{Z}[i]}$ was recently dealt with by V A Gricenko [4].

Given $a \in o$ set $N(a) := a\bar{a}$. For $0 \leqslant l \leqslant n$, a prime p in $\mathbb{N}$ and $0 \neq a \in o$ we define the double cosets

$$\mathscr{T}_n(p) := \mathscr{T}_n^o(p) := \Gamma_n^o [I^{(n)}, pI^{(n)}] \Gamma_n^o \subset \Delta_n^o(p),$$

$$\mathscr{T}_{n,l}(a) := \mathscr{T}_{n,l}^o(a) := \Gamma_n^o [I^{(n-l)}, aI^{(l)}, N(a) I^{(n-l)}, aI^{(l)}] \Gamma_n^o \subset \Delta_n^o(N(a)).$$

Now we can proceed in the same way as G Shimura [13] did (cf. also [3], IV, § 3) or follow the proofs given below in order to obtain

Theorem 5. *Let $o = \mathbb{Z}$ or let o be the ring of integers in an imaginary quadratic number field of class number one. Then the Hecke-algebra $\mathscr{H}(\Gamma_n^o, \Delta_n^o)$ is commutative and coincides with the tensor product of its primary components*

$$\mathscr{H}(\Gamma_n^o, \Delta_n^o) = \bigotimes_p \mathscr{H}(\Gamma_n^o, \Delta_{n,p}^o),$$

where p runs through all primes in $\mathbb{N}$. Given a prime p in $\mathbb{N}$, then $\mathscr{H}(\Gamma_n^o, \Delta_{n,p}^o)$ is the polynomial ring over $\mathbb{Z}$ in the following elements, which are algebraically independent:

(i) $\mathscr{T}_n(p), \quad \mathscr{T}_{n,l}(p^2), \quad l = 1, \ldots, n,$

whenever p is inert, i.e. a prime element in o,

(ii) $\mathscr{T}_n(p), \quad \mathscr{T}_{n,l}(\pi), \quad \mathscr{T}_{n,l}(\bar{\pi}), \quad l = 1, \ldots, n,$

whenever p decomposes in o and $p = \pi\bar{\pi}$ for some $\pi \in o$,

(iii) $\mathscr{T}_{n,l}(\pi), \quad l = 0, \ldots, n,$

whenever p is ramified in $\mathfrak{o}$ and associate with π^2 for some $\pi \in \mathfrak{o}$.
Especially $\mathscr{H}(\Gamma_n'', \Delta_n'')$ does not contain any zero-divisors.

3.2. *The modular group of quaternions*

In this section we deal with the corresponding situation for the modular group of quaternions over the Hurwitz order $\mathcal{O}$. Given $l \in \mathbb{N}$ and a prime p, set

$$\Delta_n(l) := \{M \in \mathrm{Mat}(2n; \mathcal{O}); \bar{M}' J M = lJ\},$$

$$\Delta_n := \bigcup_{l=1}^{\infty} \Delta_n(l), \quad \Delta_{n,p} = \bigcup_{l=0}^{\infty} \Delta_n(p^l).$$

Especially $\Gamma_n := \Delta_n(1)$ is the *modular group of quaternions of degree n*, which was investigated in [7]. Given $M \in \Delta_n$ we will always assume a block decomposition $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, where $A, B, C, D \in \mathrm{Mat}(n; \mathcal{O})$.

Let $M \in \Delta_n(l)$. Then it can be proved by induction on n from [7], II.2.2, that the right coset $\Gamma_n M$ contains a representative, whose C-block equals 0. Hence set

$$\mathscr{D}(\Gamma_n M \Gamma_n) := \left\{D; \text{ there exists } \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_n M \Gamma_n\right\},$$

$$\mathscr{B}(D, \Gamma_n M \Gamma_n) := \left\{B; \text{ there exists } \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_n M \Gamma_n\right\},$$

where $D \in \mathscr{D}(\Gamma_n M \Gamma_n)$.

Note that $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Delta_n(l)$ implies $A = l\bar{D}'^{-1}$. Given $B, B^* \in \mathscr{B}(D, \Gamma_n M \Gamma_n)$ we define $B \equiv B^* \pmod{D}$ if there exists $S \in \mathrm{Sym}(n; \mathcal{O})$ such that $B = B^* + SD$. Here $\mathrm{Sym}(n; \mathcal{O}) := \{S \in \mathrm{Mat}(n; \mathcal{O}); S = \bar{S}'\}$ denotes the set of integral Hermitian matrices. Thus one has

$$\Gamma_n \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \Gamma_n \begin{pmatrix} A & B^* \\ 0 & D \end{pmatrix} \Leftrightarrow B \equiv B^* (\mathrm{mod}\, D).$$

We can apply the same arguments, which were used for the proof of Hilfssatz IV.3.9 in [3], in order to obtain

Lemma 6

(a) *Let $M \in \Delta_n(l)$. Then a set of representatives of the right cosets in $\Gamma_n M \Gamma_n$ is given by the matrices*

$$K = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad A = l\bar{D}'^{-1},$$

where

(i) *D runs through a set of representatives of $\mathscr{U}_n \backslash \mathscr{D}(\Gamma_n M \Gamma_n)$,*

(ii) *B runs through a set of representatives of* $\bmod D$ *incongruent matrices in* $\mathscr{B}(D, \Gamma_n M \Gamma_n)$, *whenever D is given.*
One has for all $U, V \in \mathscr{U}_n$

$$\#(\mathscr{B}(D, \Gamma_n M \Gamma_n) \bmod D) = \#(\mathscr{B}(UDV, \Gamma_n M \Gamma_n) \bmod UDV).$$

(b) $\Delta_n(l)$ *decomposes into finitely many right cosets modulo* Γ_n. *Especially the pair* (Γ_n, Δ_n) *satisfies the Hecke-condition* (1).

Next we need an Elementary Divisor Theorem for the modular group. For $\mathscr{o}$ in § 3.1 two matrices in $\Delta_n(l)$ belong to the same double coset modulo $\Gamma_n^{\mathscr{o}}$ if and only if they belong to the same double coset modulo the unimodular group of degree $2n$. This is no longer true for the Hurwitz order.

Theorem 6

(a) *Given* $M \in \Delta_n(l)$ *there exist* $K_1, K_2 \in \Gamma_n, a_1, \ldots, a_n \in \mathscr{O}$ *and* $t_1, \ldots, t_n \in \mathbb{N}$ *such that*

$$K_1 M K_2 = [a_1, \ldots, a_n, t_1 a_1, \ldots, t_n a_n], \quad a_1 \| \cdots \| a_n, \quad t_\nu N(a_\nu) = l,$$

$$\nu = 1, \ldots, n. \tag{8}$$

Here $t_1, \ldots, t_n$ *are uniquely determined and* $a_1, \ldots, a_n$ *are unique up to similarity.*

(b) *Let* $n \geqslant 2$ *and suppose that two diagonal matrices* $[a_1, \ldots, a_n, t_1 a_1, \ldots, t_n a_n]$ *and* $[a_1^*, \ldots, a_n^*, t_1 a_1^*, \ldots, t_n a_n^*]$ *of the form* (8) *are given, where* a_ν *and* a_ν^* *are similar for* $\nu = 1, \ldots, n$. *Then the two matrices belong to the same double coset modulo* Γ_n.

Proof

(a) The existence of such a diagonal matrix can be proved in analogy with the proof of Theorem I.2.3 and II.2.3 in [7] and can therefore be omitted.

Hence we may assume that there is another diagonal matrix

$$[a_1^*, \ldots, a_n^*, t_1^* a_1^*, \ldots, t_n^* a_n^*], \quad a_1^* \| \cdots \| a_n^*, \quad t_\nu^* N(a_\nu^*) = 1, \quad \nu = 1, \ldots, n,$$

in the same double coset. In the case $n = 1$ we apply [7], II.2.6, in order to see that $t_1 = t_1^*$ and $a_1^* = \varepsilon a_1 \delta$ for some $\varepsilon, \delta \in \mathscr{E}$.

Therefore let $n \geqslant 2$. The elementary divisor form of M is given by

$$[a_1, \ldots, a_{n-1}, x, y, t_{n-1} a_{n-1}, \ldots, t_1 a_1],$$

where $[x, y]$ is the elementary divisor form of $[a_n, t_n a_n]$. The uniqueness under unimodular equivalence yields the similarity of a_ν and a_ν^* as well as of t_ν and t_ν^* for $\nu = 1, \ldots, n-1$. Due to [9], Theorem 4, we may assume that $a_\nu = a_\nu^*$ and $t_\nu = t_\nu^*$ hold for $\nu = 1, \ldots, n-1$.

Let $M = [a_1, \ldots, a_n, t_1 a_1, \ldots, t_n a_n]$, $M^* = [a_1, \ldots, a_{n-1}, a_n^*, t_1 a_1, \ldots, t_{n-1} a_{n-1}, t_n^* a_n^*]$. We use the fact that M and M^* belong to the same double coset. In view of [7], I.2.4, we can therefore choose L and $K = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n$ as well as $U \in \mathscr{U}_n$ such that

$$LM[U, \tilde{U}^{t-1}] = M^* K, \tag{*}$$

where the n-th column of A has the form $(0, \ldots, 0, a)'$ for some $a \in \mathscr{O}$.

Denote the gcrd of the n-th column in $(*)$ by g (cf. [7], I, § 1). If $(c_1,\dots,c_n)'$ stands for the n-th column of C, we obtain $\bar{a}c_n=\bar{c}_n a$ from the fundamental relations for symplectic matrices. In view of [7], II.2.4. and II.2.6, there exist $\alpha,\gamma\in\mathbb{Z}$ and $v\in\mathcal{O}$ such that $a=\alpha v$ and $c_n=\gamma v$. Thus the n-th column of the right hand side in $(*)$ equals

$$(0,\dots,0,\alpha a_n^* v, t_1 a_1 c_1,\dots,t_{n-1}a_{n-1}c_{n-1},\gamma t_n^* a_n^* v)'.$$

The condition (8) leads to $a_n^*|t_\nu$ for $\nu=1,\dots,n-1$. Choose an element $d\in\mathcal{O}$, which is a right divisor of a_n^*v and similar to a_n^*. Then $d|_r g$ follows.

If $(u_1,\dots,u_n)'$ denotes the n-th column of U, then [7], I.2.8, implies $g=\operatorname{gcrd}(a_1u_1,\dots,a_nu_n)$. At first one easily checks $\operatorname{inv}(g)|\operatorname{inv}(a_n)$. Next $\operatorname{inv}(a_n^*)=\operatorname{inv}(d)|\operatorname{inv}(g)|\operatorname{inv}(a_n)$ and the symmetry yield $\operatorname{inv}(a_n)=\operatorname{inv}(a_n^*)$. On the other hand we can choose $x_1,\dots,x_n\in\mathcal{O}$ such that $x_1a_1u_1+\cdots+x_na_nu_n=\operatorname{inv}(a_n)^{-1}N(a_n)$ in view of $\operatorname{gcrd}(u_1,\dots,u_n)=1$. Hence $g|\operatorname{inv}(a_n)^{-1}N(a_n)$ follows. This leads to $a_n^*|\operatorname{inv}(a_n)^{-1}N(a_n)$. In virtue of $\operatorname{inv}(a_n^*)=\operatorname{inv}(a_n)$ we conclude $N(a_n^*)|N(a_n)$. The symmetry yields $N(a_n^*)=N(a_n)$ and thus the similarity of a_n and a_n^*. Finally $l=t_nN(a_n)=t_n^*N(a_n^*)$ implies $t_n=t_n^*$.

(b) The assertion follows from [9], Theorem 4. □

3.3. *The decomposition into primary components*

The crucial part is contained in

PROPOSITION 5

Let $n\geqslant 2$, $L\in\Delta_n(l)$ and $M\in\Delta_n(m)$, where $l,m\in\mathbb{N}$ are relatively prime. Then one has

$$(\Gamma_n L\Gamma_n)\cdot(\Gamma_n M\Gamma_n)=\Gamma_n LM\Gamma_n.$$

Proof. Choose representatives of the right cosets $L_0=\begin{pmatrix}A_0 & B_0\\ 0 & D_0\end{pmatrix}$ resp. $M_1=\begin{pmatrix}A_1 & B_1\\ 0 & D_1\end{pmatrix}$ in $\Gamma_nL\Gamma_n$ resp. $\Gamma_nM\Gamma_n$ according to Lemma 6 and $K^*=\begin{pmatrix}A^* & 0\\ 0 & D^*\end{pmatrix}\in\Delta_n(lm)$ in the form (8) such that $L_0M_1=NK^*$ holds for some $N\in\Gamma_n$. Then it follows that $N=\begin{pmatrix}\bar{U}'^{-1} & 0\\ 0 & U\end{pmatrix}\begin{pmatrix}I & S\\ 0 & I\end{pmatrix}$ holds for appropriate $U\in\mathcal{U}_n$ and $S\in\operatorname{Sym}(n;\mathcal{O})$. At first $D_0D_1=UD^*$ and Proposition 3 lead to $U=I$ and to unique diagonal forms D_0 and D_1. Then we have $A_0B_1+B_0D_1=SD_0D_1$. If $A_0=[a_1,\dots,a_n]$ and $D_1=[d_1,\dots,d_n]$ we conclude that the entries $b_{\nu\mu}$ of B_1 belong to $\operatorname{Tor}(a_\nu,d_\mu)$. Since l,m are relatively prime, $\operatorname{Tor}(a_\nu,d_\mu)=\mathcal{O}d_\mu$ and thus $b_{\nu\mu}=0$ follow. Clearly $B_0=SD_0$ leads to $B_0=0$ in view of Lemma 6. Then Theorem 6 completes the proof. □

Now we can apply the same arguments as for the proof of Theorem 2 in order to obtain

Theorem 7. *Let $n\geqslant 2$, then $\mathcal{H}(\Gamma_n,\Delta_n)$ is commutative and coincides with the tensor products of its primary components, i.e.*

$$\mathcal{H}(\Gamma_n,\Delta_n)=\bigotimes_p\mathcal{H}(\Gamma_n,\Delta_{n,p}),$$

where p runs through all primes in $\mathbb{N}$.

Just as for the unimodular group the case $n=1$ has to be excluded. Note that

$$(\Gamma_1(aI)\Gamma_1)\cdot(\Gamma_1 M\Gamma_1)=\Gamma_1(aM)\Gamma_1=(\Gamma_1 M\Gamma_1)\cdot(\Gamma_1(aI)\Gamma_1)$$

holds for $0\neq a\in\mathcal{O}$ and $M\in\mathrm{Mat}(2;\mathbb{Z})$, $\det M>0$. Now we can apply [7], II.2.6, and Lemma 2 in order to obtain

Remark 2

The Hecke-algebra $\mathscr{H}(\Gamma_1,\Delta_1)$ is not commutative. More precisely one has

$$\mathscr{H}(\Gamma_1,\Delta_1)=\mathscr{H}(\mathscr{U}_1,\mathscr{M}_1)\otimes\mathscr{H}(\Gamma_1^{\mathbb{Z}},\Delta_1^{\mathbb{Z}}).$$

3.4. *The primary components*

In view of Theorem 7 we may restrict ourselves to the primary components. At first we deal with the case $p=2$. In view of Theorem 6 each double coset $\Gamma_n M\Gamma_n\in\Delta_n(2^q)$ possesses a unique representative

$$M=[(1+i)^{l_1},\ldots,(1+i)^{l_n},(1+i)^{l_1}2^{q-l_1},\ldots,(1+i)^{l_n}2^{q-l_n}],$$
$$0\leqslant l_1\leqslant\cdots\leqslant l_n\leqslant q.$$

We define the double cosets

$$\mathscr{T}_l^{(n)}(1+i):=\Gamma_n[I^{(n-l)},(1+i)I^{(l)},2I^{(n-l)},(1+i)I^{(l)}]\Gamma_n\subset\Delta_n(2).$$

Given $M\in\Delta_n(2)$ one has the obvious criterion

$$M\in\mathscr{T}_l^{(n)}(1+i)\Leftrightarrow r_2(M)=n-l.$$

Now let $n\geqslant 2$ and p be an odd prime. Choose a completely primitive $\pi\in\mathscr{N}(p)$. In view of Theorem 6 each double coset $\Gamma_n M\Gamma_n\subset\Delta_n(p^q)$ possesses a unique representative

$$M=[\pi^{l_1}p^{m_1},\ldots,\pi^{l_n}p^{m_n},\pi^{l_1}p^{q-l_1-m_1},\ldots,\pi^{l_n}p^{q-l_n-m_n}],$$
$$0\leqslant l_\nu,\quad 0\leqslant m_\nu,\quad l_\nu+m_\nu\leqslant m_{\nu+1},\quad l_n+2m_n\leqslant q. \tag{9}$$

Thus there exist two double cosets in $\Delta_n(p)$. namely

$$\mathscr{S}_n(p):=\Gamma_n[I^{(n)},pI^{(n)}]\Gamma_n,\quad \mathscr{S}_n^*(p):=\Gamma_n[I^{(n-1)},\pi,pI^{(n-1)},\pi]\Gamma_n.$$

Note that the matrices in $\mathscr{S}_n(p)$ and $\mathscr{S}_n^*(p)$ are unimodularly equivalent. Given $M\in\Delta_n(p)$ one has the criterion

$$M\in\mathscr{S}_n(p)\Leftrightarrow\{\det\check{D};D\in\mathscr{D}(\Gamma_n M\Gamma_n)\}\subset\{p^{2l};0\leqslant l\leqslant n\},$$
$$M\in\mathscr{S}_n(p)\Leftrightarrow\{\det\check{D};D\in\mathscr{D}(\Gamma_n M\Gamma_n)\}\subset\{p^{2l-1};1\leqslant l\leqslant n\}. \tag{10}$$

Clearly one has

$$\mathscr{D}(\mathscr{S}_n(p))=\bigcup_{l=0}^{n}R_{2l}^{(n)}(p),\quad \mathscr{D}(\mathscr{S}_n^*(p))=\bigcup_{l=1}^{n}R_{2l-1}^{(n)}(p). \tag{11}$$

Furthermore we state all the double cosets in $\Delta_n(p^2)$, namely

$$\mathscr{R}_{2l}^{(n)}(p) := \Gamma_n[I^{(n-l)}, pI^{(l)}, p^2 I^{(n-l)}, pI^{(l)}]\Gamma_n, \quad 0 \leqslant l \leqslant n,$$

$$\mathscr{R}_{2l-1}^{(n)}(p) := \Gamma_n[I^{(n-l)}, \pi, pI^{(l-1)}, p^2 I^{(n-l)}, p\pi, pI^{(l-1)}]\Gamma_n, \quad 1 \leqslant l \leqslant n,$$

$$\mathscr{R}_{*}^{(n)}(p) := \Gamma_n[I^{(n-1)}, \pi^2, p^2 I^{(n-1)}, \pi^2]\Gamma_n.$$

Obviously one has

$$M \in \mathscr{R}_l^{(n)}(p) \Rightarrow r_p(M) = 2n - l, \quad M \in \mathscr{R}_*^{(n)}(p) \Rightarrow r_p(M) = 2n. \tag{12}$$

If $M \in \Delta_n(p^2)$ satisfies $r_p(M) = 2n$ one has the additional criterion

$$M \in \mathscr{R}_*^{(n)}(p) \Leftrightarrow \mathscr{D}(\Gamma_n M \Gamma_n) \cap \{G \in \mathscr{M}_n; pG^{-1} \in \mathrm{Mat}(n; \mathcal{O})\} = \varnothing. \tag{13}$$

Next observe that $\#(\mathscr{B}(D, \Delta_n(p)) \bmod D)$ equals

$$p^{l(2l-1)} \quad \text{if } D = [I^{(n-l)}, pI^{(l)}], \quad 0 \leqslant l \leqslant n,$$

$$p^{(l-1)(2l-1)} \quad \text{if } D = [I^{(n-l)}, \pi, pI^{(l-1)}], \quad 1 \leqslant l \leqslant n.$$

Then we can apply Lemma 6, (10), (11), (12) and (13) and proceed in the same way as in the proof of Lemma 5 in order to obtain

PROPOSITION 6

Let $n \geqslant 2$ and p be an odd prime. Then one has

(a)
$$\deg \mathscr{S}_n(p) = \sum_{l=0}^{n} E_{2l}^{(2n)}(1, p, \ldots, p^{2n-1}),$$

$$\deg \mathscr{S}_n^*(p) = \sum_{l=1}^{n} E_{2l-1}^{(2n)}(1, p, \ldots, p^{2n-1}).$$

(b)
$$\mathscr{S}_n(p)^2 = \mathscr{R}_0^{(n)}(p) + \sum_{l=1}^{n} \deg \mathscr{S}_l(p) \mathscr{R}_{2l}^{(n)}(p),$$

$$\mathscr{S}_n^*(p)^2 = \mathscr{R}_*^{(n)}(p) + \sum_{l=1}^{n} \deg \mathscr{S}_l^*(p) \mathscr{R}_{2l}^{(n)}(p),$$

$$\mathscr{S}_n(p) \cdot \mathscr{S}_n^*(p) = \sum_{l=1}^{n} \left(\sum_{m=1}^{l} E_{2m-1}^{(2l-1)}(1, p, \ldots, p^{2l-2}) \right) \mathscr{R}_{2l-1}^{(n)}(p).$$

Now we can state the structure theorem.

Theorem 8

(a) *$\mathscr{H}(\Gamma_n, \Delta_{n,2})$ is the polynomial ring over $\mathbb{Z}$ in $n+1$ elements*

$$\mathscr{T}_0^{(n)}(1+i), \ldots, \mathscr{T}_n^{(n)}(1+i),$$

which are algebraically independent.

$$\mathscr{S}_n(p), \mathscr{S}_n^*(p), \mathscr{R}_2^{(n)}(p), \ldots, \mathscr{R}_{2n}^{(n)}(p),$$

which are algebraically independent. Especially $\mathscr{H}(\Gamma_n, \Delta_n)$ does not contain any zero-divisors.

Proof. Again we only prove (b), since (a) can be treated in the same way. Let $\mathscr{A}$ denote the subalgebra of $\mathscr{H}(\Gamma_n, \Delta_{n,p})$ generated by the double cosets quoted above. We show by induction on q that the $\mathbb{Z}$-submodule $\mathscr{H}(\Gamma_n, \Delta_n(p^q))$ is contained in $\mathscr{A}$.

This is obvious for $q = 0, 1$ and follows from Proposition 6 for $q = 2$. Therefore let $q \geqslant 3$. Now we show successively that all the double cosets $\Gamma_n M \Gamma_n \subset \Delta_n(p^q)$ with $r_p(M) = r$ belong to $\mathscr{A}$. Again $r = 0$ is obvious, since we can "divide" by $\mathscr{R}_{2n}^{(n)}(p) = \Gamma_n(pI)\Gamma_n$. Assume $r > 0$ and that the representative M has the form (9). Then we compute the product of $\mathscr{R}_{2n-r}^{(n)}(p)$ with

$$\Gamma_n[1, \ldots, 1, \pi^{l_{s+1}} p^{m_{s+1}-1}, \ldots, \pi^{l_n} p^{m_n-1}, p^{q-2}, \ldots, \pi^{l_n} p^{q-l_n-m_n-1}]\Gamma_n,$$

if $m_1 = \cdots = m_s = l_1 = \cdots = l_s = 0$, $m_{s+1} > 0$, $0 < r = 2s \leqslant 2n$,

$$\Gamma_n[1, \ldots, 1, \pi^{l_s-1}, \pi^{l_{s+1}} p^{m_{s+1}-1}, \ldots, \pi^{l_n} p^{m_n-1}, p^{q-2}, \ldots, \pi^{l_n} p^{q-l_n-m_n-1}]\Gamma_n,$$

if $m_1 = \cdots = m_s = l_1 = \cdots = l_{s-1} = 0$, $l_s > 0$, $r = 2s - 1$.

In the case $m_1 = \cdots = m_n = l_1 = \cdots = l_{n-1} = 0$, $l_n > 0$, $r = 2n$, we calculate

$$\mathscr{S}_n^*(p) \cdot \Gamma_n[1, \ldots, 1, \pi^{l_n-1}, p^{q-1}, \ldots, p^{q-1}, \pi^{l_n-1} p^{q-l_n}]\Gamma_n.$$

The same methods as used in the proof of Theorem 3 show that the product equals $T + \Gamma_n M \Gamma_n$, where T is a linear combination of double cosets $\Gamma_n L \Gamma_n$ satisfying $L \in \Delta_n(p^q)$ and $r_p(L) < r$. Thus the induction hypothesis yields $\mathscr{A} = \mathscr{H}(\Gamma_n, \Delta_{n,p})$.

In order to demonstrate the algebraical independence, we use (9) and calculate

$$\begin{aligned}
\dim \mathscr{H}(\Gamma_n, \Delta_n(p^q)) &= \#\{(m_1, l_1, \ldots, m_n, l_n)^t \in \mathbb{N}_0^{2n}; l_\nu + m_\nu \leqslant m_{\nu+1}, l_n + 2m_n \leqslant q\} \\
&= \#\{(q_1, \ldots, q_{2n})^t \in \mathbb{N}_0^{2n}; 0 \leqslant q_1 \leqslant \cdots \leqslant q_{2n}, q_{2n-1} + q_{2n} \leqslant q\} \\
&= \sum_{r=0}^{[q/2]} \#\{(q_1, \ldots, q_{2n-2}, r, q_{2n})^t \in \mathbb{N}_0^{2n}; 0 \leqslant q_1 \leqslant \cdots \leqslant q_{2n-2} \leqslant r \leqslant q_{2n} \leqslant q - r\} \\
&= \sum_{r=0}^{[q/2]} (q + 1 - 2r) \binom{2n - 2 + r}{r}, \qquad (*)
\end{aligned}$$

where $[q/2]$ is the greatest integer, which does not exceed $q/2$. On the other hand a monomial

$$\mathscr{S}_n(p)^{\nu_0} \cdot \mathscr{S}_n^*(p)^{\nu_1} \cdot \mathscr{R}_2^{(n)}(p)^{\nu_2} \cdot \ldots \cdot \mathscr{R}_{2n}^{(n)}(p)^{\nu_{2n}}, \quad \nu_l \in \mathbb{N}_0,$$

belongs to $\mathscr{H}(\Gamma_n, \Delta_n(p^q))$ if and only if

$$\nu_0 + \nu_1 + 2\nu_2 + \cdots + 2\nu_{2n} = q.$$

Elementary combinatorics show that the number of these monomials also equals (*). Since the double cosets generate $\mathscr{H}(\Gamma_n, \Delta_{n,p})$, they prove to be algebraically independent. □

Remark 3. Let $n \geqslant 2$ and p be an odd prime. Consider the $\mathbb{Z}$-submodule $\mathscr{A}_{n,p}$ of $\mathscr{H}(\Gamma_n, \Delta_{n,p})$ consisting of all formal linear combinations, where the coefficients of $\Gamma_n M \Gamma_n$ and $\Gamma_n N \Gamma_n$ coincide, whenever $\mathscr{U}_{2n} M \mathscr{U}_{2n} = \mathscr{U}_{2n} N \mathscr{U}_{2n}$. A careful look at the proof of the theorem above shows that $\mathscr{A}_{n,p}$ becomes a subalgebra of $\mathscr{H}(\Gamma_n, \Delta_{n,p})$ and that $\mathscr{A}_{n,p}$ equals the polynomial ring over $\mathbb{Z}$ in $2n+1$ elements

$$\mathscr{S}_n(p) + \mathscr{S}_n^*(p), \quad \mathscr{R}_1^{(n)}(p), \ldots, \mathscr{R}_{2n}^{(n)}(p),$$

which are algebraically independent.

4. The law of interchange with the Siegel ϕ-operator

In this paragraph we investigate the homomorphism of the Hecke-algebras, which describes the law of interchange between Hecke-operators and the Siegel ϕ-operator. The meaning of this homomorphism is emphasized by the fact that the theory of stable modular forms combined with this law of interchange yields the invariance of the subspace spanned by theta-series under certain Hecke-operators (cf. [3], [7], [18]).

4.1. *The definition*

In this section we deal with o from §3.1 and the Hurwitz order $\mathcal{O}$ simultaneously. Denote the corresponding Hecke-algebra over $\mathbb{Q}$ by

$$\tilde{\mathscr{H}}(\Gamma_n, \Delta_n) := \mathscr{H}(\Gamma_n, \Delta_n) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Moreover let r be an integer, which is divisible by the number of units in o resp. even for the Hurwitz order. Let

$$n \geqslant 2, \quad M \in \Delta_n \quad \text{and} \quad L = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in \Delta_{n-1}.$$

Then $\mathscr{C}(M, L)$ denotes the set of right cosets in $\Gamma_n M \Gamma_n$, which possess a representative of the form

$$M^* = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A = \begin{pmatrix} A_1 & 0 \\ \bar{a}' & \alpha \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & b \\ \bar{b}_1' & \beta \end{pmatrix},$$

$$C = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} D_1 & d \\ 0 & \delta \end{pmatrix}, \tag{*}$$

where a, b, b_1, d are column vectors of length $n-1$. Considering only representatives of the form (*), we set

$$\phi_r(\Gamma_n M \Gamma_n) = \sum_{L: \Gamma_{n-1} \backslash \Delta_{n-1} / \Gamma_{n-1}} \left(\sum_{M^*: \Gamma_n \backslash \mathscr{C}(M,L)} \delta^{-r} \right) \Gamma_{n-1} L \Gamma_{n-1}$$
$$\in \tilde{\mathscr{H}}(\Gamma_{n-1}, \Delta_{n-1})$$

for $\mathfrak{o}$ resp.

$$\phi_r(\Gamma_n M \Gamma_n) = \sum_{L:\Gamma_{n-1}\backslash\Delta_{n-1}/\Gamma_{n-1} \in \hat{\mathscr{H}}(\Gamma_{n-1},\Delta_{n-1})} \left(\sum_{M^*:\Gamma_n\backslash\mathscr{G}(M,L)} N(\delta)^{-r/2} \right) \Gamma_{n-1} L \Gamma_{n-1}$$

for the Hurwitz order. The assumptions on r ensure that ϕ_r is well-defined. Linear extension yields a map

$$\phi_r : \hat{\mathscr{H}}(\Gamma_n, \Delta_n) \to \hat{\mathscr{H}}(\Gamma_{n-1}, \Delta_{n-1}),$$

which proves to be a homomorphism of the $\mathbb{Q}$-algebras (cf. [3], IV, § 4).

4.2. *The case of the Hermitian modular group*

In the case of the Hermitian modular group we can use Theorem 5 and proceed in the same way as in [8] in order to obtain

Theorem 9. *Let $\mathfrak{o}$ be the ring of integers in an imaginary quadratic number field of class number one and let r be an integral multiple of the number of units in $\mathfrak{o}$. Given $n \geqslant 2$ and a prime number $p \in \mathbb{N}$, the following holds*

(i) *If p is inert, one has*

$$\phi_r(\mathscr{T}_n(p)) = (1 + p^{2n-1-r})\mathscr{T}_{n-1}(p),$$

$$\phi_r(\mathscr{T}_{n,l}(p)) = \sum_{\substack{m=l-1,l,l+1 \\ 0 \leqslant m \leqslant n-1}} t_m \mathscr{T}_{n-1,m}(p)$$

for $0 \leqslant l \leqslant n$, where

$$t_{l-1} = p^{2n-2l-r}, \quad t_l = 1 + (p-1)p^{2n-2l-2-r} + p^{4n-2-2r},$$

$$t_{l+1} = (p^{2l+2} - 1)(p^{2l+1} + 1)p^{2n-2l-3-r}.$$

(ii) *If p decomposes and $N(\pi) = p$ holds for some $\pi \in \mathfrak{o}$, one has*

$$\phi_r(\mathscr{T}_n(p)) = (1 + p^{2n-1-r})\mathscr{T}_{n-1}(p) + p^n \bar{\pi}^{-r}\mathscr{T}_{n-1,1}(\pi) + p^n \pi^{-r}\mathscr{T}_{n-1,1}(\bar{\pi}),$$

$$\phi_r(\mathscr{T}_{n,l}(\pi)) = \sum_{\substack{m=l-1,l,l+1 \\ 0 \leqslant m \leqslant n-1}} t_m \mathscr{T}_{n-1,m}(\pi)$$

for $1 \leqslant l \leqslant n$, where

$$t_{l-1} = p^{n-l}\pi^{-r}, \quad t_l = 1 + p^{2n-1-r}, \quad t_{l+1} = p^{n+l}\bar{\pi}^{-r}.$$

(iii) *If p is ramified and associate to π^2 for some $\pi \in \mathfrak{o}$, one has*

$$\phi_r(\mathscr{T}_{n,l}(\pi)) = \sum_{\substack{m=l-1,l,l+1 \\ 0 \leqslant m \leqslant n-1}} t_m \mathscr{T}_{n-1,m}(\pi)$$

for $0 \leqslant l \leqslant n$, *where*

$$t_{l-1} = p^{n-l}\pi^{-r}, \quad t_l = 1 + p^{2n-1-r}, \quad t_{l+1} = (p^{2l+2} - 1)p^{n-l-2}\pi^{-r}.$$

Using [8] resp. [21] as well as Theorems 5 and 9, we obtain

COROLLARY 2

Let $o = \mathbb{Z}$ *and* $r \in \mathbb{Z}$ *be even or let* o *be the ring of integers in an imaginary quadratic number field of class number one and let* $r \in \mathbb{Z}$ *be a multiple of the number of units in* o. *If* $n \geqslant 2$ *the homomorphism*

$$\phi_r : \hat{\mathscr{H}}(\Gamma_n^o, \Delta_n^o) \to \hat{\mathscr{H}}(\Gamma_{n-1}^o, \Delta_{n-1}^o)$$

becomes surjective.

4.3. *The law of interchange for the modular group of quaternions*

We start with the description of the simplest cases.

Lemma 7. Let r *be even integer*

(a) *If* $n \geqslant 2$ *one has*

$$\phi_r(\mathscr{T}^{(n)}(1+i)) = \sum_{\substack{m=l-1,l,l+1 \\ 0 \leqslant m \leqslant n-1}} t_m \mathscr{T}_m^{(n-1)}(1+i)$$

for $0 \leqslant l \leqslant n$, *where*

$$t_{l-1} = 2^{2n-2l-r/2}, \quad t_l = 1 + 2^{4n-3-r}, \quad t_{l+1} = (2^{2l+4} - 1)2^{2n-2l-4-r/2}.$$

Especially the homomorphism

$$\phi_r : \hat{\mathscr{H}}(\Gamma_n, \Delta_{n,2}) \to \hat{\mathscr{H}}(\Gamma_{n-1}, \Delta_{n-1,2})$$

becomes surjective.

(b) *Let* $n \geqslant 3$ *and* p *be an odd prime. Then one has*

$$\phi_r(\mathscr{S}_n(p)) = (1 + p^{4n-3-r})\mathscr{S}_{n-1}(p) + (p+1)p^{2n-2-r/2}\mathscr{S}_{n-1}^*(p),$$
$$\phi_r(\mathscr{S}_n^*(p)) = (p+1)p^{2n-2-r/2}\mathscr{S}_{n-1}(p) + (1 + p^{4n-3-r})\mathscr{S}_{n-1}^*(p).$$

Proof

(a) The assertion can be proved in the same way as in [8].

(b) Let $\pi \in \mathscr{N}(p)$. We quote representatives of $\Gamma_n \backslash \mathscr{C}(N, L)$ in the form $M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$, $A = p\bar{D}'^{-1}$. Set $K^{(n)} = [I^{(n)}, pI^{(n)}]$, $K_*^{(n)} = [I^{(n-1)}, \pi, pI^{(n-1)}, \pi]$. If $N = K^{(n)}$ and $L = K^{(n-1)}$ we have

$$D = \begin{pmatrix} pI & 0 \\ 0 & 1 \end{pmatrix}, \quad B = 0, \quad I = I^{(n-1)} \quad \text{and} \quad D = pI^{(n)}, \quad B = \begin{pmatrix} 0 & b \\ \bar{b}' & \beta \end{pmatrix},$$

where $b:(\mathcal{O}/p\mathcal{O})^{n-1}$ and $\beta = 0, \ldots, p-1$. Thus there are $p^{4n-3}+1$ representatives. In the case $N = K^{(n)}$ and $L = K_*^{(n-1)}$ we have

$$D = \begin{pmatrix} pI & 0 & 0 \\ 0 & \pi & \gamma \\ 0 & 0 & \delta \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & b \\ 0 & 0 & \beta \\ \delta\bar{b}' & \beta^* & \beta_0 \end{pmatrix}, \quad \beta^* = \bar{\delta}^{-1}\bar{\beta}\pi, \quad I = I^{(n-2)},$$

where $b:(\mathcal{O}/\delta\mathcal{O})^{n-2}, \beta, \gamma:\mathrm{Tor}(\bar{\pi}, \delta)/\mathcal{O}\delta$, $\beta_0 \in \mathcal{O}$ is fixed satisfying $\bar{\gamma}\beta + \bar{\delta}\beta_0 \in \mathbb{Z}$ and $\delta:\mathscr{E}\backslash\mathscr{N}(p)$. Hence there are $(p+1)p^{2n-2}$ matrices. In the case $N = K_*^{(n)}$ and $L = K^{(n-1)}$ we obtain $(p+1)p^{2n-2}$ representatives in the form

$$D = \begin{pmatrix} pI & 0 \\ 0 & \delta \end{pmatrix}, \quad B = \begin{pmatrix} 0 & b \\ \delta\bar{b}' & 0 \end{pmatrix}, \quad I = I^{(n-1)},$$

where $b:(\mathcal{O}/\delta\mathcal{O})^{n-1}$ and $\delta:\mathscr{E}\backslash\mathscr{N}(p)$. Finally for $N = K_*^{(n)}$ and $L = K_*^{(n-1)}$ we have exactly $p^{4n-3}+1$ representatives

$$D = \begin{pmatrix} pI & 0 & 0 \\ 0 & \pi & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = 0 \quad \text{and}$$

$$D = \begin{pmatrix} pI & 0 & 0 \\ 0 & \pi & \pi\delta \\ 0 & 0 & p \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & 0 & b \\ 0 & 0 & \pi\beta \\ \bar{b}' & \bar{\beta} & -\bar{\delta}\beta + s \end{pmatrix}, \quad I = I^{(n-2)},$$

where $b:(\mathcal{O}/p\mathcal{O})^{n-2}$, $\delta, \beta:\mathcal{O}/\bar{\pi}\mathcal{O}$ and $s = 0, \ldots, p-1$. □

Given an odd prime p we define

$$\mathscr{T}_n(p) := \sum_{M:\Gamma_n\backslash\Delta_n(p)/\Gamma_n} \Gamma_n M \Gamma_n.$$

In $n \geqslant 2$ one has $\mathscr{T}_n(p) = \mathscr{S}_n(p) + \mathscr{S}_n^*(p)$. Then we can apply the lemma above and a simple additional consideration for $n = 2$ in order to obtain

COROLLARY 3

Let $n \geqslant 2$, p be an odd prime and r an even integer. Then one has

$$\phi_r(\mathscr{T}_n(p)) = (p^{2n-1-r/2}+1)(p^{2n-2-r/2}+1)\mathscr{T}_{n-1}(p).$$

Finally we consider the general case, which surprisingly contains two exceptions.

Theorem 10. *Let $n \geqslant 3$, p be an odd prime and r an even integer. Then the homomorphism*

$$\phi_r:\mathscr{H}(\Gamma_n, \Delta_n) \to \mathscr{H}(\Gamma_{n-1}, \Delta_{n-1})$$

is surjective except for $r = 4n-2$ and $r = 4n-4$. In the latter cases one has more

precisely

$$\phi_r(\hat{\mathscr{H}}(\Gamma_n, \Delta_n)) = \mathbb{Q}[\mathscr{T}_n(p), \mathscr{R}_1^{(n)}(p), \ldots, \mathscr{R}_{2n}^{(n)}(p)].$$

Proof. Since a cancellation of rows and columns does not increase the rank of a matrix, (12) yields

$$\phi_r(\mathscr{R}_l^{(n)}(p)) = \sum_{m=l-2}^{2n-2} t_m \mathscr{R}_m^{(n-1)}(p), \quad 3 \leqslant l \leqslant 2n,$$

with certain $t_m \in \mathbb{Q}$. It is easy to see that $t_{l-2} > 0$ holds and an explicit calculation yields $t_{l-2} = p^{4n-2l-r}$. The same description as in the proof of Lemma 7 moreover **leads** to

$$\phi_r(\mathscr{R}_2^{(n)}(p)) = p^{4n-4-r}(\mathscr{R}_0^{(n-1)}(p) + \mathscr{R}_*^{(n-1)}(p)) + \sum_{m=1}^{2n-2} t_m \mathscr{R}_m^{(n-1)}(p)$$

for some $t_m \in \mathbb{Q}$.

Then we note that $1 + p^{4n-3-r} = (p+1)p^{2n-2-r/2}$ holds for even $r \in \mathbb{Z}$ if and only if $r = 4n-4$ or $r = 4n-2$. Now a combination of Lemma 7, Proposition 6 and Theorem 8 completes the proof. □

Note that in the exceptional weights the arising subalgebra was characterized in Remark 3. The applications to the theory of modular forms will be described in a forthcoming paper [10].

Acknowledgements

The paper was prepared during the author's stay at the Tata Institute of Fundamental Research in Bombay under the Indo-German Cultural Exchange Programme. The author would like to express his thanks to Professor S Raghavan and the Tata Institute for their kind hospitality as well as to both DAAD (Germany) and U.G.C. (India) for sponsoring the visit.

References

[1] Apostol T M, *Introduction to analytic number theory* (New York, Berlin, Heidelberg, Tokyo: Springer-Verlag) (1976)

[2] Braun H, Hermitian modular functions I, II, III, *Ann. Math.* **50** (1949), 827–855; *Ann. Math.* **51** (1950) 92–104; *Ann. Math.* **53** (1951) 143–160

[3] Freitag E, *Siegelsche Modulfunktionen* (Berlin, Heidelberg, New York: Springer-Verlag) (1983)

[4] Gricenko VA, *The Maaß-space for* SU(2, 2), *Hecke-operators and zeta-functions* (Russian), preprint series LOMI R-7-85, Leningrad (1985)

[5] Hurwitz A, *Vorlesungen über die Zahlentheorie der Quaternionen* (Berlin: Springer-Verlag) (1919)

[6] Jacobson N, *Basic algebra I* (San Francisco: Freeman) (1974)

[7] Krieg A, *Modular forms on half-spaces of quaternions, Lecture Notes in Math.* 1143 (Berlin, Heidelberg, New York, Tokyo: Springer-Verlag) (1985)

[8] Krieg A, Das Vertauschungsgesetz zwischen Hecke-Operatoren und dem Siegelschen ϕ-Operator, *Arch. Math.* **46** (1986) 323–329

[9] Krieg A, The elementary divisor theory over the Hurwitz order of integral quaternions, *Linear and Multilinear algebra* **21** (1987) 325–344

[10] Krieg A, *Hecke-operators with respect to the modular group of quaternions* (in preparation)
[11] Maaß H, Die Primzahlen in der Theorie der Siegelschen Modulfunktionen, *Math. Ann.* **124** (1951) 87–122
[12] Newman M, *Integral matrices* (New York, London: Academic Press) (1972)
[13] Shimura G, On modular correspondences for $Sp(N, \mathbb{Z})$ and their congruence relations, *Proc. Natl. Acad. Sci.* **49** (1963) 824–828
[14] Shimura G. *Introduction to the arithmetic theory of automorphic functions* (Tokyo and Princeton: Iwanami Publishers and Princeton University Press) (1971)
[15] Siegel C L, Einführung in die Theorie der Modulfunktionen n-ten Grades, *Math. Ann.* **116** (1939) 617–657; *Ger. Abh.* II, 97–137
[16] Tamagawa T, On the ζ-functions of a division algebra, *Ann. Math.* **77** (1963) 387–405
[17] Thompson R C, *Invariant factors of integral quaternion matrices* (Santa Barbara) (1986) (preprint)
[18] Vasudevan T C, *Some problems on hermitian modular forms*, thesis, Bombay 1978
[19] Vignéras M F, *Arithmétique des Algèbres de Quaternions, Lecture Notes in Math.* 800, (Berlin, Heidelberg, New York: Springer-Verlag) (1980)
[20] Weil A, On the analogue of the modular group in characteristic P, in F E Browder, *Functional analysis and related fields*, (Berlin, Heidelberg, New York: Springer-Verlag) (1970)
[21] Zharkovskaya N A, The Siegel operator and Hecke operators, *Funct. Anal. Appl.* **8** (1974) 113–120

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 231–237.
© Printed in India.

Poincaré series for $SO(n, 1)$

JIAN-SHU LI†, I PIATETSKI-SHAPIRO and P SARNAK*

† Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

* The Institute for Advanced Studies, The Hebrew University of Jerusalem, Givat Ram 91904, Jerusalem, Israel

Abstract. A theory of Poincaré series is developed for Lobachevsky space of arbitrary dimension. For a general non-uniform lattice a Selberg-Kloosterman zeta function is introduced. It has meromorphic continuation to the plane with poles at the corresponding automorphic spectrum. When the lattice is a unit group of a rational quadratic form, the Selberg-Kloosterman zeta function is computed explicitly in terms of exponential sums. In this way a non-trivial Ramanujan-like bound analogous to "Selberg's 3/16 bound" is proved in general.

Keywords. Poincaré series; Lobachevsky space; Selberg-Kloosterman zeta function; non-uniform lattices.

1. Introduction

The theory of holomorphic Poincaré series has been developed and studied quite generally [11]. It allows one to construct explicitly holomorphic cusp forms and to study their Fourier coefficients. Non-holomorphic Poincaré series were introduced by Selberg [10] for $SL(2, \mathbb{R})$. By expanding these series once spectrally in $L^2(\Gamma \backslash SL(2, \mathbb{R})/K)$ and once directly in a Fourier series in a cusp, one obtains a relation between the L^2 spectrum and sums of Kloosterman sums. In this way using bounds on Kloosterman sums due to Weil, Selberg established the well-known estimate

$$\lambda_1 \geqslant 3/16 \tag{1}$$

for the second smallest eigenvalue of the Laplacian for any congruence subgroup of $SL(2, \mathbb{R})$. The bound (1) goes part of the way towards the 'Ramanujan Conjecture', $\lambda_1 \geqq 1/4$, which remains a basic outstanding problem; (see Iwaniec [5] for some recent progress).

The above relation and set-up has numerous striking applications [4] which we do not enter into here. Suffice it to say that it is desirable to develop such a theory for more general groups. For $GL(n)$, $n \geqq 3$, computations have been done by Bump–Friedberg–Goldfeld [1] and Stevens [12]. However, it appears that direct estimation of the resulting exponential sums does not produce results better than what follows from property T.

In this note we describe results for $G = SO(n, 1)$. We will obtain the meromorphic continuation to $\mathbb{C}$ of the 'Kloosterman-Selberg' zeta function for arbitrary $\Gamma \subseteq G$ as well as the analogue of (1) for congruence subgroups of unit groups of rational quadratic forms. Detailed proofs will appear elsewhere.

2. General non-uniform lattices

Let G be the real orthogonal group of a form of signature $(r+1,1)$, $r \geqq 2$, i.e. $G = SO(r+1,1)$. We realize G as

$$G = \left\{ g \in SL_{r+2} \;\middle|\; {}^t g \begin{pmatrix} & & 1 \\ & I_r & \\ 1 & & \end{pmatrix} g = \begin{pmatrix} & & 1 \\ & I_r & \\ 1 & & \end{pmatrix} \right\}, \tag{2}$$

where I_r is the $r \times r$ identity matrix. Denote by A, H and U the subgroups

$$A = \left\{ \begin{pmatrix} a & & \\ & I_r & \\ & & a^{-1} \end{pmatrix} \;\middle|\; a \in \mathbb{R}^* \right\} \tag{3}$$

$H = SO_r$, the standard orthogonal group which we embedded in G via

$$h \to \begin{pmatrix} 1 & & \\ & h & \\ & & 1 \end{pmatrix},$$

$$U = \left\{ \begin{pmatrix} 1 & -{}^t u & -\frac{1}{2}\langle u, u \rangle \\ & I_r & {}^t u \\ & & 1 \end{pmatrix} : u \in \mathbb{R}^r \right\} \tag{5}$$

where u is thought of as a column vector and $\langle\ ,\ \rangle$ is the usual inner product on $\mathbb{R}^r$.

Then $P = UAH$ is a parabolic subgroup of G with unipotent radical $U \cong \mathbb{R}^r$ and Levi component $M = AH$.

Let $\Gamma \subseteq G$ be a discrete subgroup of finite covolume but not compact. We may take one of its cusps to correspond to U i.e. $\Gamma \cap U = \Gamma_\infty$ is a lattice of full rank in U. For simplicity assume that in fact $\Gamma \cap P = \Gamma_\infty$ and that this is the only cusp subgroup of Γ. We fix non-trivial additive characters ψ, η of Γ_∞ (i.e. ψ, η are members of the lattice dual to Γ_∞ in $\mathbb{R}^r$). The Bruhat decomposition of G asserts that

$$G = P \cup PwU \tag{6}$$

where $w = \begin{pmatrix} & & -1 \\ & I_r & \\ 1 & & \end{pmatrix}$. In this way we may write every $\gamma \in \Gamma$, $\gamma \notin P$ uniquely as

$$\gamma = u(\gamma)a(\gamma)h(\gamma)wv(\gamma), \quad \text{or}$$

$$= u(\gamma)m(\gamma)wv(\gamma) \tag{7}$$

with the obvious notation concerning membership.

Correspondingly let

$$M(\Gamma) = \{m(\gamma) | \gamma \in \Gamma - \Gamma_\infty\}.$$

One may then choose a set of representatives for $\gamma \in \Gamma_\infty \backslash \Gamma / \Gamma_\infty$, $\gamma \notin \Gamma_\infty$ in the form

$$umwv, \tag{8}$$

where for each $m \in M(\Gamma)$, u and v run over a finite set in $U \times U$. The 'Kloosterman sum' $\mathrm{Kl}(\psi, \eta, m)$ for $m \in M(\Gamma)$ is defined by

$$\mathrm{Kl}(\psi, \eta, m) = \sum \psi(u)\eta(v), \tag{9}$$

where the sum ranges over the u and v above. Let τ be an irreducible (finite dimensional) unitary representation of H, we define the 'Kloosterman–Selberg' zeta function by

$$Z(\psi, \eta, \tau, s) = \sum_{m \in M(\Gamma)} \mathrm{Kl}(\psi, \eta, m)\tau(h_m)|a_m|^{s+r/2}. \tag{10}$$

By comparing this series with the Eisenstein series (corresponding to Γ_∞) it follows that the series converges absolutely for $\mathrm{Re}(s) > r/2$.

Theorem 1: *$Z(\psi, \eta, \tau, s)$ extends to a meromorphic function in s in the entire plane. Furthermore the poles of Z may be explicitly described in terms of the automorphic spectrum (representations) of $L^2(\Gamma\backslash G)$. In particular it is analytic in $\mathrm{Re}(s) \geqq r/2$ and has only finitely many poles in $\mathrm{Re}(s) > 0$—these latter will be referred to as exceptional poles (or spectrum).*

In order to describe briefly the precise location of poles as well as the method of proof we consider the case of $r = 2$. In this case $G \cong SL(2, \mathbb{C})$. This case contains the essential features. Changing our notation slightly we have $P = UAH$ with

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \mathbb{C} \right\}, \quad A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| a \in \mathbb{R}^* \right\}, \quad H \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \right\}.$$

Hence $M = AH = \left\{ \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \middle| z \in \mathbb{C}^* \right\}$ and we identify M with $\mathbb{C}^*$ by $\begin{pmatrix} z & \\ & z^{-1} \end{pmatrix} \leftrightarrow z$.
The irreducible representations of H correspond to integers $r \in \mathbb{Z}$. Let b_1, b_2 be smooth radial functions of compact support on $\mathbb{C}$ and $\mathbb{C}^*$ respectively. Define the function f on G by

$$f(u_1 w u_2 z) = \psi(u_1) b_1(|u_2|) b_2(|z|) \left(\frac{z}{|z|} \right)^r$$
$$= 0 \quad \text{if } g \text{ is not of the above form.} \tag{11}$$

Here $u_1, u_2 \in U$, $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $z \in M$ and ψ (and later η) are characters as before. The Poincaré series $P_f(g)$ on G is defined by

$$P_f(g) = \sum_{\Gamma_\infty \backslash \Gamma} f(\gamma g). \tag{12}$$

The series (12) consists of only a finite number of non-zero terms and in fact $P_f(g)$ is Γ-automorphic and in $C_0^\infty(\Gamma\backslash G)$ (i.e. smooth of compact support). For $\mathrm{Re}(s)$ large consider

$$I = \int_{\mathbb{C}^*} \int_{\Gamma_\infty \backslash U} P_f(uz)\bar{\eta}(u)\, \mathrm{d}u \left(\frac{(z)}{|z|} \right)^r |z|^s \, \mathrm{d}^* z. \tag{13}$$

A calculation shows that

$$I = \left(\int_{\mathbb{C}^*} b_2(|z|)|z|^s d^*z\right) \times \sum_{n=0}^{\infty} \frac{(i\pi)^{2n}|\xi|^{2n}}{(n!)^2} \int_{\mathbb{C}^*} b_1(|u|)|u|^{2n} du.\, Z(\psi, \eta, 4+s+2n, r) \tag{14}$$

where $\eta(u) = \exp[-\pi i(\xi u + \xi u)]$ and for $\nu \in \mathbb{Z} = \hat{H}$

$$Z(\psi, \eta, \nu, s) = \sum_{\alpha \in \bar{M}(\Gamma)} K_1(\psi, \eta, \alpha)\left(\frac{\alpha}{|\alpha|}\right)^{\nu} |\alpha|^s. \tag{15}$$

Note that due to the slightly different parametrization of G, $Z(\psi, \eta, \nu, s)$ converges absolutely for $\mathrm{Re}(s) > 4$. Theorem 1 in this case, that is the meromorphic continuation and location of poles of Z follows immediately from (13), (14) and

Lemma 2: Let $\Theta \in C_0^\infty(\Gamma\backslash G)$. Then

$$\int_{\mathbb{C}^*} \int_{\Gamma_\infty \backslash U} \Theta(uz)\psi(u)\, du \left(\frac{z}{|z|}\right)^{-r} |z|^s d^*z$$

is meromorphic in $\mathbb{C}$ with possible poles at the poles of $L_{\pi \times \chi_r}((s/4)+(1/2))$, where π runs through the discrete irreducible constituents of $L^2(\Gamma\backslash G)$, as well as the poles of the Eisenstein series $E(g,(s/4)+(1/2))$. Here χ is the character $(z/|z|)^r$ of $\mathbb{C}^*$ and $L_\pi(s)$ is the local L-function corresponding to π (see Jacquet-Langlands [6]) which is a product of two-gamma functions.

In particular the first infinite set of poles of $Z(\psi, \eta, \nu, s)$ is along the line $\mathrm{Re}(s) = 2$ corresponding to the discrete occurrences of weight r representations of G appearing in $L^2(\Gamma\backslash G)$. Lemma 2 is proved by expanding Θ spectrally and using the theory of Whittaker functions.

3. Lower bounds for λ_1

In order to obtain a lower bound for exceptional spectrum (i.e. analogue of (1)) we restrict our attention to Γ's which are congruence subgroups of unit groups of rational quadratic forms. This is necessary since in fact the bound we obtain, see Corollary 4, is false for general Γ (see the comments at the end of this section). For simplicity of exposition we stick to the algebraic group G defined in (2). Let G be the subgroup of G whose entries are integers (i.e. a unit group) and for $D \geqslant 1$ an integer we let $\Gamma(D)$ be the congruence subgroup $\Gamma(D) = \{g \in G \mid g \equiv 1 \pmod{D}\}$. $\Gamma(D)$ is a non-uniform lattice in $G(r \geqslant 3)$. At this point it is both convenient and essential in our approach to work adelically. So we let A be the adele ring over Q and let $G(A)$, $G(Q)$, $P(A)$, $P(Q)$, $U(A)$, $U(Q)\ldots$, etc, be the adelic, respectively Q, points of the corresponding subgroups. Let $\psi = \prod_p \psi_p$ be a standard character of $Q\backslash A$. For $\xi \in (1/D)\mathbb{Z}^r$ we define a character ψ^ξ of $U(Q)\backslash U(A)$ by

$$\psi^\xi(u) = \psi(\langle u, \xi \rangle), \quad u \in U(A). \tag{16}$$

Clearly we may decompose ψ^ξ as $\psi^\xi = \prod_p \psi_p^\xi$. To introduce Poincaré series on

$G(Q)\backslash G(A)$ we define functions $f^{\xi}(g)$, $g\in G(A)$ as follows:

(a) For $p=\infty$ we set

$$f^{\xi}_{\infty}(uyk)=\psi^{\xi}_{\infty}(u)y^{s+r/2}\exp(-2\pi|\xi|y),$$

where $u\in U(R)$, $y\in A(R)$, $k\in K_{\infty}$ and uyk is the Iwasawa decomposition. Note here that this is a somewhat different choice to (11) above and that it corresponds to τ the identity representation of H.

(b) For $p<\infty$, let

$$K_p=\{g\in G(\mathbb{Z}_p)\,|\,g\equiv 1 \bmod p^l \quad \text{where} \quad p^l\| D\}.$$

Set $f^{\xi}_{p}(uk)=\psi^{\xi}_{p}(u)$, $u\in U(Q_p)$, $k\in K_p$ and $f^{\xi}_{p}(g)=0$ for g outside the open set $U(Q_p)K_p$. Define

$$f^{\xi}(g)=\prod_{p} f^{\xi}_{p}(g_p), \quad g=(g_{\infty},g_2,\ldots)\in G(A).$$

Now f^{ξ} satisfies

$$f^{\xi}(ug)=\psi^{\xi}(u)f^{\xi}(g).$$

Finally the Poincaré series $P_{\xi}(g,s)$ is defined by

$$P_{\xi}(g,s)=\sum_{\gamma\in U(Q)\backslash G(Q)} f^{\xi}(\gamma g). \tag{17}$$

Again by comparison with the Eisenstein series we find that the series (17) converges absolutely for $\mathrm{Re}(s)>r/2$. An inspection shows that the function $P_{\xi}(g,s)$ really lives on $\Gamma(D)\backslash G(R)/K_{\infty}$. As before we consider

$$I(\xi,s)=\int_{U(Q)\backslash U(A)} P_{\xi}(ug,s)\psi^{\xi}(-u)\,\mathrm{d}u. \tag{18}$$

A calculation as before relates $I(\xi,s)$ to the following Kloosterman-Selberg zeta function: For $p<\infty$, $\mathrm{Kl}_p(\xi,\xi,\gamma)$ for $\gamma\in M(Q)$, is the local "Kloosterman integral" (it is a sum in fact)

$$\mathrm{Kl}_p(\xi,\xi,\gamma)=\int_{U(Q_p)} f^{\xi}_{p}(\xi wu)\psi^{\xi}_{p}(-u)\,\mathrm{d}u. \tag{19}$$

For example if $\gamma=ah\in M(Q)$ with $|h|_p=|a|_p>1$, where $|h|_p=\max_{ij}(|h_{ij}|_p)$, then

$$\mathrm{Kl}_p(\gamma)=\sum_{\lambda\in(\mathbb{Z}_p/a^{-1}\mathbb{Z}_p)^*}\psi^{\xi}_{p}\left(\lambda u_0+\frac{1}{\lambda}v_0\right) \tag{19'}$$

for suitable $u_0,v_0\in U(Q_p)$, $|u_0|_p=|v_0|_p=|a|_p$. (19') is a classical one-dimensional Kloosterman sum over the field with p elements. In the other cases $\mathrm{Kl}_p(\gamma)$ is more complicated being an exponential sum in more than one variable.

The Kloosterman sum corresponding to $\gamma \in M(A)$ is

$$\mathrm{Kl}(\xi, \xi, \gamma) = \prod_{p < \infty} \mathrm{Kl}_p(\xi, \xi, \gamma). \tag{20}$$

The Kloosterman zeta function is

$$Z(\xi, \xi, s) = \sum_{\gamma \in M(Q)} \mathrm{Kl}(\xi, \xi, \gamma) |a_\gamma|^{s+r/2}. \tag{21}$$

This zeta function is of course a special case of those introduced in § 2 (corresponding to $\Gamma = \Gamma(D)$) but as it appears here the Kl's are factored naturally over the primes. This is the reason the adelic approach was taken since with this factorization nontrivial estimates on $\mathrm{Kl}(\xi, \xi, \gamma)$ can be made via ones for $\mathrm{Kl}_p(\xi, \xi, \gamma)$.

The precise relation between $I(\xi, s)$ and $Z(\xi, \xi, s)$ is that in $\mathrm{Re}(s) > \frac{1}{2}r - 1$ they have the same poles. On the other hand by spectrally decomposing $P_\xi(g)$ one can determine the precise location of poles of $I(\xi, s)$. To state the result we let $\Theta_j(g)$, $j = 1, \ldots, R$ be a basis of eigenfunctions of Δ (the Laplacian) on $\Gamma(D) \backslash G(R)/K_\infty$ which are exceptional, i.e. their eigenvalues $\lambda_j = (\frac{1}{2}r - \nu_j)(\frac{1}{2}r + \nu_j)$ satisfy $0 < \lambda_j < (\frac{1}{2}r)^2$, or what is the same ν_j is real and $\nu_j > 0$.

PROPOSITION 3:

$I(\xi, s)$ has simple poles at $s = \nu_j$ and positive residue if the ξth Fourier coefficient of θ_j is non-zero.

We now come to the main point.

Theorem 4: *$Z(\xi, \xi, s)$ is holomorphic in $\mathrm{Re}(s) > \frac{1}{2}(r - 1)$.*

This is proved by appealing to the definition of $Z(\xi, \xi, s)$ in (21) and estimating the terms $\mathrm{Kl}(\xi, \xi, \gamma)$. The $\mathrm{Kl}_p(\xi, \xi, \gamma)$ of the form (19') are estimated (when they are non-trivial) by Weil's bound [13] while all other Kl_p's are estimated by a trivial volume bound.

To obtain the result one needs to carefully examine those γ's for which $f^\xi(\gamma w u) \neq 0$ for some u. In this way one is able to control the contribution from those terms which are estimated trivially.

From the above considerations we obtain the following analogue of (1) (see also [9] for the case $SL_2(\sigma) \subset SL_2(C)$ where σ is the ring of integers in an imaginary quadratic field).

COROLLARY 5:

If λ_1 is the second smallest ($\lambda_0 = 0$) eigenvalue of Δ on $L^2(\Gamma(D) \backslash G(R)/K_\infty)$ then

$$\lambda_1 \geqq \tfrac{1}{2}(r - \tfrac{1}{2}).$$

In this context the analogue of the "Ramanujan conjecture" would be the assertion that $\lambda_1 \geqq (\frac{1}{2}r)^2$ (for $\Gamma(D)$), that is there is no exceptional spectrum. Corollary 4 says that to some extent this conjecture is true, however, we note that for $r \geqq 3$ it is in fact false. One can construct discrete exceptional spectrum on $\Gamma(D) \backslash G(R)/K_\infty$ (even cuspidal) with $\lambda = \frac{1}{2}r - 1, \frac{1}{2}r - 3 \ldots$. This phenomenon is similar to what happens for

half integral weight for $SL(2)^{\sim}$. In fact the above exceptional forms are constructed by lifting holomorphic cusp forms for $SL(2)^{\sim}$ (or $SL(2)$ depending on the parity of r) to $\Gamma(D)\backslash G(R)$. These 'counter examples' are similar to those constructed by Howe and Piatetski-Shapiro [3].

To conclude we note that the above analysis and results hold equally well for any unit group of a rational quadratic form. Also similar non-trivial estimates for the representation parameters occurring in $L_0^2(G(Q)\backslash G(A))$ at places p other than ∞ may be derived in a similar way as long as G_p is still rank 1. (The other cases represent no problem in view of property T). For a treatment of the theory at finite places over $GL(2)$ and for a general introduction to the $GL(2)$ adelic Poincaré series, see Piatetski-Shapiro [7].

Finally, note that Theorem 3 does not hold for all Γ. Using deformation argument as in [10, 8] one may construct Γ's with λ_1 as small as we please. Of course such Γ's cannot be congruence groups.

Acknowledgement

We would like to thank J Bernstein for numerous suggestions and insights.

Note: Some results similar to those obtained here were announced recently by Elstrodt Grunewald and Mennicke [2]. Their methods however seem different to those presented here.

References

[1] Bump D, Friedberg S and Goldfeld D, Poincaré series and Kloosterman sums for $SL(3, \mathbb{Z})$ (preprint)
[2] Elstrodt J, Grunewald F and Mennicke J, Poincaré series, Kloosterman sums and eigenvalues of the Laplacian for congruence groups acting on hyperbolic spaces (preprint) (1987)
[3] Howe R and Piatetski-Shapiro I, A counterexample to the generalized Ramanujan conjecture for (quasi-)split groups, *Proc. Symp. Pure Math.* **23** (1979) 315–322
[4] Iwaniec H, International Congress of Mathematics, Talk; Berkeley (1986)
[5] Iwaniec H, Small-eigenvalues for $L^2(\Gamma_0(p)\backslash H, \lambda_p)$ (preprint) (1987)
[6] Jacquet H and Langlands R, Automorphic forms on $GL(2)$, *Lecture Notes in Math*, 114 Springer (1970)
[7] Piatetski-Shapiro I, Kloosterman sums over functional fields (in preparation)
[8] Randol B, Small eigenvalues of the Laplace operator on compact Riemann surfaces, *Bull. Am. Math. Soc.* **80** (1974) 996–1000
[9] Sarnak P, The arithmetic and geometry of some hyperbolic three manifolds, *Acta. Math.* **151** (1983) 253–295
[10] Selberg A, On the estimation of Fourier coefficients of modular forms, *Proc. Symp. Pure Math.* **8** (1965) 1–15
[11] Siegel C L, *Lectures on advanced analytic number theory* (Bombay: Tata Institute of Fundamental Research) (1961)
[12] Stevens G, Poincaré series on $GL(m)$ and Kloosterman sums, *Math. Ann.* **277** (1987) 25–51
[13] Weil A, On some exponential sums, *Proc. Natl. Acad. Sci.* **34** (1948) 204–207

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 239–245.
© Printed in India.

Fluctuations in the mean of Euler's phi function

HUGH L MONTGOMERY*
Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

Abstract. We consider the error term in the mean value estimate of Euler's phi function $\varphi(n)$, and show that it is $\Omega_{\pm}(x(\log\log x)^{\frac{1}{2}})$. This improves on the earlier results of Pillai and Chowla, and of Erdös and Shapiro.

Keywords. Euler's phi function; fluctuations; mean value estimate.

1. Statement of results

Let $\varphi(n)$ denote Euler's totient function, which counts the number of reduced residue classes (mod n). We study the remainder term in the asymptotic function

$$\sum_{n\leqslant x}\varphi(n) = (3/\pi^2)x^2 + R(x). \tag{1}$$

Dirichlet showed that $R(x) \ll x^{1+\varepsilon}$ for any $\varepsilon > 0$, and Mertens [5] refined this to $R(x) \ll x\log x$. More recently, Walfisz [12] improved this to $R(x) \ll x(\log x)^{2/3}(\log\log x)^{4/3}$. For most x, $R(x)$ is not much larger than $O(x)$, since Pillai and Chowla [7] have shown that

$$\sum_{n\leqslant x} R(n) \sim \frac{3}{2\pi^2}x^2, \tag{2}$$

while Chowla [1] found that

$$\int_0^x R(u)^2\,du \sim (6\pi^2)^{-1}x^3. \tag{3}$$

Instead of $R(x)$, some authors have considered the remainder $R_0(x)$ defined by the relation

$$\sum_{n\leqslant x}\varphi(n)/n = (6/\pi^2)x + R_0(x). \tag{4}$$

Pillai and Chowla [7] showed that $R(x)$ and $R_0(x)$ are closely linked. We formulate this in the following refined form.

*Research supported in part by the National Science Foundation Grant NSF-DMS-85-02804.

Theorem 1. *For $x \geqslant 2$,*

$$R_0(x) = R(x)/x + O(\exp(-c\sqrt{\log x})). \tag{5}$$

Here c is a positive absolute constant.

Sylvester [9], [10] conjectured that $R(x) > 0$ whenever x is a positive integer, but this was disproved by Sarma [8], who showed that $R(820) < 0$. In fact $R(n) > 0$ and $R_0(n) > 0$ for $n < 820$, while $R(820) = -9{\cdot}092\ldots$ and $R_0(820) = -0{\cdot}012\ldots$. Karl K Norton [6, pp. 86–87] made the interesting observation that Sylvester [10] tabulated $\varphi(n)$, $\sum_{m \leqslant n} \varphi(m)$, and $(3/\pi^2)n$ for $n = 1, 2, \ldots, 1000$, but failed to note that $R(820) < 0$. Pillai and Chowla [7] showed that

$$R(x) = \Omega(x \log\log\log x). \tag{6}$$

That $R(x)$ changes sign infinitely often was finally proved by Erdös and Shapiro [3], who demonstrated that

$$R(x) = \Omega_{\pm}(x \log\log\log\log x). \tag{7}$$

We now improve on these latter estimates.

Theorem 2. *Let $R(x)$ be determined by* (1). *Then*

$$R(x) = \Omega_{\pm}(x\sqrt{\log\log x}).$$

Concerning the maximum order of magnitude of $R(x)$, we conjecture that

$$R(x) \ll x \log\log x \tag{8}$$

and that

$$R(x) = \Omega_{\pm}(x \log\log x). \tag{9}$$

From the construction of Pillai and Chowla [7] one sees that $\varphi(n)$ can be small, say $\varphi(n) < n/4$, for all n in an interval $x < n < x + c \log\log\log x$. However, in intervals longer than this $\varphi(n)$ has the expected mean value, since it may be shown that if $2 \leqslant h \leqslant x$ then

$$(6/\pi^2)h + O(\log h) + O(\log\log\log x) \leqslant \sum_{x < n \leqslant x+h} \varphi(n)/n \leqslant (6/\pi^2)h + O(\log h).$$

This is a slight refinement of Theorem 6 of Erdös [2].

2. Basic lemmas

In the discussion below we take $s(x)$ to be the 'saw tooth' function. That is, $s(x)$ has period 1, $s(0) = 0$, and $s(x) = 1/2 - x$ for $0 < x < 1$.

Lemma 1. We have

$$R_0(x) = \tfrac{1}{2}\varphi(x)/x + \sum_{d \leqslant y} \mu(d)s(x/d)/d + O(\exp(-c_1\sqrt{\log x})) \tag{10}$$

uniformly for $x \geqslant 2, y \geqslant x\exp(-c_1\sqrt{\log x})$.

Here we set $\varphi(x) = 0$ if x is not an integer. The constants c_i are positive and absolute. The method of Walfisz [12, Chapter IV] can be used to show that (10) holds in the larger range $y \geqslant x^{\eta}$, for any given $\eta > 0$, but such a strengthening of the lemma would have no impact on our main results.

Proof. We first establish (10) in the case $y = x$. We recall that $\varphi(n)/n = \sum_{d|n}\mu(d)/d$. But if $f(n) = \sum_{d|n}g(d)$, then

$$\sum_{n \leqslant x} f(n) = x \sum_{d \leqslant x} g(d)/d - \sum_{d \leqslant x} g(d)\{x/d\}. \tag{11}$$

Thus in particular,

$$\sum_{n \leqslant x} \varphi(n)/n = x \sum_{d \leqslant x} \mu(d)/d^2 - \sum_{d \leqslant x} \mu(d)\{x/d\}/d.$$

Here the first sum on the right, if extended over all $d \geqslant 1$, would be $1/\zeta(2) = 6/\pi^2$. Hence we see that

$$R_0(x) = x \sum_{d \geqslant x} \mu(d)/d^2 - \sum_{d \leqslant x} \mu(d)\{x/d\}/d.$$

Put $L(x) = \sum_{d \leqslant x}\mu(d)/d$. By a variant of the quantitative form of the prime number theorem we know that $L(x) \ll \exp(-c_0\sqrt{\log x})$ for $x \geqslant 2$. Thus the first sum above is

$$-L(x)/x + \int_x^{\infty} L(u)/u^2\,\mathrm{d}u \ll \frac{1}{x}\exp(-c_0\sqrt{\log x})).$$

Using this, and also adding $L(x)/2$ to the expression, we see that

$$R_0(x) = \sum_{d \leqslant x} \mu(d)(1/2 - \{x/d\})/d + O(\exp(-c_0\sqrt{\log x})).$$

But $1/2 - \{x\} = s(x)$ if x is not an integer. We note that if x/d is an integer then x is an integer and $d|x$. In the case that x is an integer, these d combine to contribute an amount $\frac{1}{2}\varphi(x)/x$. Thus we have (10) with $c_1 = c_0$ when $y = x$.

To establish (10) when $y > x$ it suffices to note that

$$\sum_{x < d \leqslant y} \mu(d)s(x/d)/d = \left(\frac{1}{2} - \frac{x}{y}\right)L(y) + \tfrac{1}{2}L(x) - \int_x^y L(u)/u^2\,\mathrm{d}u$$

$$\ll \exp(-c_0\sqrt{\log x}).$$

We now consider y in the range $x\exp(-c_1\sqrt{\log x}) \leqslant y \leqslant x$. Suppose that k is a

positive integer, $1 \leqslant k \leqslant x/y$. Then $s(x/d)$ is monotonic for $x/(k+1) < d < x/k$, so that

$$\sum_{x/(k+1)<d<x/k} \mu(d)s(x/d)/d \ll \exp(-\tfrac{1}{2}c_0\sqrt{\log y}).$$

On summing this over $1 \leqslant k \leqslant x/y$ we find that

$$\sum_{y<d\leqslant x} \mu(d)s(x/d)/d \ll xy^{-1}\exp(-\tfrac{1}{2}c_0\sqrt{\log y}).$$

This suffices to give (10) with $c_1 = c_0/4$.

Lemma 2. Let b and $r > 0$ be relatively prime integers, and let β be a real number. Then

$$\sum_{n=1}^{r} s(bn/r + \beta) = s(r\beta). \tag{12}$$

Proof. Both sides are periodic with period $1/r$, so we may assume that $0 \leqslant \beta < 1/r$. The numbers bn run through a complete residue system (mod r), so we may assume that $b = 1$. If $\beta = 0$ then the left hand side is

$$\sum_{n=1}^{r-1} s(n/r) = \sum_{n=1}^{r-1} (1/2 - n/r) = 0.$$

If $0 < \beta < 1$ then the sum is

$$\sum_{n=0}^{r-1} s(n/r + \beta) = \sum_{n=0}^{r-1} (1/2 - n/r - \beta) = 1/2 - r\beta.$$

Thus (12) holds in all cases.

We now consider a sum as in (12), but extended over an arbitrary interval $1 \leqslant n \leqslant N$. The size of such a sum depends in a complicated way on the continued fraction of b/r, but the following crude estimate is sufficient for our present purpose.

Lemma 3. Let b and $r > 0$ be relatively prime integers, and let β be a real number. Then for any positive N,

$$\sum_{n=1}^{N} s(nb/r + \beta) \ll \frac{N}{r}s(r\beta) + O(r). \tag{13}$$

Proof. Write $N = Qr + R$, $0 \leqslant R < r$. By Lemma 2 the above is

$$Qs(r\beta) + \sum_{n=1}^{R} s(nb/r + \beta).$$

Here the first term is $(N/r)s(r\beta) + O(1)$, and the second term is $\ll R \ll r$.

Lemma 4. If q is a positive integer, $q \leqslant \exp(c_2\sqrt{\log N})$, α is a non-integral real number, $0 < \alpha < q$, then

$$\sum_{n=1}^{N} R_0(nq + \alpha) = C(q, \alpha)N + O(N\exp(-c_2\sqrt{\log N})). \tag{14}$$

where

$$C(q,\alpha)=\frac{6}{\pi^2}\left(\prod_{p|q}(1-p^{-2})\right)^{-1}\sum_{d|q}\mu(d)s(\alpha/d)/d. \tag{15}$$

This estimate is substantially equivalent to Theorem 3.1 of Erdős and Shapiro [3], although both the formulation of the result and the proof are quite different. With more work we could establish an estimate of this sort for larger q, but it would not affect our main results. By taking $q=1$, $\alpha=0^+$, we find that

$$\sum_{n=1}^{N}R_0(n)=(3/\pi^2)N+O(N\exp(-c\sqrt{\log N})),$$

a result similar to (2).

Proof. We apply Lemma 1 with $y=(N+1)q\exp(-c_1\sqrt{\log N})$. The sum of the error term in (10) contributes an amount $\ll N\exp(-c_1\sqrt{\log N})$, so it suffices to consider the double sum

$$\sum_{n=1}^{N}\sum_{d\leqslant y}\mu(d)s((nq+\alpha)/d)/d. \tag{16}$$

We invert the order of summation and apply Lemma 3 with $r=d/(d,q)$, $\beta=\alpha/d$. Thus the inner sum is

$$\sum_{n=1}^{N}s((qn+\alpha)/d)=(d,q)s(\alpha/(d,q))N/d+O(d).$$

The error term here, when inserted in (16), contributes an amount $\ll y$, which is acceptable in (14) if we take $c_2=c_1/3$. We may suppose that d is square-free, and then write $d=ef$ with $e|q$, $(f,q)=1$. Thus the main term above contributes to (16) the amount

$$N\sum_{e|q}\mu(e)s(\alpha/e)/e\sum_{\substack{f\leqslant y/e\\(f,q)=1}}\mu(f)/f^2.$$

If we delete the constraint $f\leqslant y/e$ in the inner sum then the above becomes $C(q,\alpha)N$. In making this change the inner sum is altered by an amount $\ll e/y$, which introduces an error term

$$\ll 2^{\omega(q)}N/y\ll(2^{\omega(q)}/q)\exp(c_1\sqrt{\log N})\ll N\exp(-c_1\sqrt{\log N}).$$

3. Proof of theorem 1

Proof. We recall that $\sum\varphi(n)/n^s=\zeta(s-1)/\zeta(s)$ for $\sigma>1$. Thus by a familiar Mellin transform,

$$\sum_{n\leqslant x}\left(1-\frac{n}{x}\right)\varphi(n)/n=\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{\zeta(s)x^s}{\zeta(s+1)s(s+1)}\,ds \tag{17}$$

for $a > 1$. Let $\mathscr{C}$ denote the contour $\sigma = -c/\log\tau$, $-\infty < t < +\infty$, where $\tau = |t| + 4$. Then $1/\zeta(s+1) \ll \log\tau$ and $\zeta(s) \ll \tau^{1/2}\log\tau$ on this contour, so that

$$\int_{\mathscr{C}} \cdots \ll \exp(-c\sqrt{\log x}).$$

In the region between $\mathscr{C}$ and the original line of integration, the integrand is regular, apart from a simple pole at $s = 1$ with residue $(3/\pi^2)x$. Thus the expression (17) is $(3/\pi^2)x + O(\exp(-c\sqrt{\log x}))$. But from (1) and (4) we see easily that the left hand side is $(3/\pi^2)x + R_0(x) - R(x)/x$, so we have the stated result.

By treating the identity

$$\sum_{n\leqslant x}(x-n)\varphi(n) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{\zeta(s-1)x^{s+1}}{\zeta(s)s(s+1)}\,ds$$

similarly, we find that

$$\int_0^x R(u)\,du \ll x^2\exp(-c\sqrt{\log x}).$$

Thus we see that the main term in (2) is due to the fact that the remainder term is summed, rather than integrated. If in (2) we were to replace $R(n)$ by $R(n^-)$, then the sign of the main term would be reversed on the right hand side.

4. Proof of theorem 2

In view of Theorem 1, it suffices to show that $R_0(x) = \Omega_{\pm}(\sqrt{\log\log x})$. We apply Lemma 4 with q taken to be the product of all primes $p \equiv 3 \pmod 4$ for which $p \leqslant z$. Here $z \approx \sqrt{\log N}$ is chosen so that $\omega(q)$ is even, which is to say $q \equiv 1 \pmod 4$, and so that $q \leqslant \exp(c_2\sqrt{\log x})$. If $d \mid q$, then $q/d \equiv 1$ or $3 \pmod 4$ according as $\omega(d)$ is even or odd. That is, $\mu(d)s(q/(4d)) = 1/4$ for all $d \mid q$, so that

$$C(q, q/4) \approx \sum_{d\mid q}\mu^2(d)/d \approx \sqrt{\log z} \approx \sqrt{\log\log N}.$$

Thus by taking $\alpha = q/4$ in Lemma 4 we see that there are x for which $R_0(x)$ is large and positive. Since $C(q, 3q/4) = -C(q, q/4)$, we take $\alpha = 3q/4$ to obtain the result with the negative sign.

The construction above, of q for which $\mu(d)$ and $s(q/(4d))$ are correlated, is modelled after the work of Lehmer [4], who showed that there exist q for which

$$\max_N \left|\sum_{\substack{n=1\\(n,q)=1}}^{N} 1 - \varphi(q)N/q\right| \geqslant 2^{\omega(q)-2}.$$

Vijayaraghavan [11] showed that there exist q for which the above quantity is $> 2^{\omega(q)-1} - \delta$, for any $\delta > 0$, but in his constructions $\varphi(q)/q$ is very near 1. In the present context we want $\varphi(q)/q$ to be as small as possible.

References

[1] Chowla S D, Contributions to the analytic theory of numbers, *Math. Z.* **35** (1932) 279–299
[2] Erdős P, Some remarks about additive and multiplicative functions, *Bull. Am. Math. Soc.* **52** (1946) 527–537
[3] Erdős P and Shapiro H N, On the changes of sign of a certain error function, *Can. J. Math.* **3** (1951) 375–385
[4] Lehmer D H, The distribution of totatives, *Can. J. Math.* **7** (1955) 347–357
[5] Mertens F, Ueber einige asymptotische gesetze der zahlen-theorie, *J. Reine Angew. Math.* **77** (1874) 289–338
[6] Norton K K, Numbers with small prime factors, and the least kth power non-residue, *Mem. Am. Math. Soc.* **106** (1971) pp. 106
[7] Pillai S S and Chowla S D, On the error terms in some asymptotic formulae in the theory of numbers (I), *J. London Math. Soc.* **5** (1930) 95–101
[8] Sarma M L N, On the error term of a certain sum, *Proc. Indian Acad. Sci.* **A3** (1936) 338
[9] Sylvester J J, Sur le nombre de fractions ordinaires enégales qu'un peut exprimer en se servant de chiffres qui n'excedent pas un nombre donné, *C.R. Acad. Sci, Paris* **96** (1883) 409–413; *Mathematical papers* (Cambridge: University Press) Vol. 4, pp. 84–87 (1912)
[10] Sylvester J J, On the number of fractions contained in the Farey series of which the limiting number is given, *Philos. Mag.* **15** (1883) 251–257; **16** (1883) 230–233; *Mathematical papers* (Cambridge: University Press) Vol. 4 pp. 101–109 (1912)
[11] Vijayaraghavan T, On a problem in elementary number theory, *J. Indian Math. Soc.* **15** (1951) 51–56
[12] Walfisz A, Weylsche Exponentialsummen in der neueren Zahlentheorie, *Math. forschungsberichte* (Berlin: Deutcher Verlag Wiss) p. 231 (1963)

On the supersingular reduction of elliptic curves

M RAM MURTY*
Department of Mathematics, McGill University, 805 Sherbrooke Street West, Montreal, Canada H3A 2K6

Abstract. Let $a \in Q$ and denote by E_a the curve $y^2 = (x^2 + 1)(x + a)$. We prove that $E_a(F_p)$ is cyclic for infinitely many primes p. This fact was known previously only under the assumption of the generalized Riemann hypothesis.

Keywords. Supersingular reduction, elliptic curves.

Let E be an elliptic curve defined over Q. For all but finitely many primes p, E has good reduction (mod p) and it makes sense to consider E (mod p). It is classical (see [1]) that the ring $\mathrm{End}_{\bar{F}_p}(E)$ of algebraic endomorphisms defined over $\bar{F}_p$ has Z-rank 2 or 4. In the latter case, E is said to have supersingular reduction (mod p). Our first result is:

Theorem 1. *Let E be an elliptic curve defined over Q and suppose that E has supersingular reduction* (mod p). *Then the 2-complement of $E(F_p)$ is cyclic.*

The interest of Theorem 1 lies in the following. In 1976, Lang and Trotter [4] formulated the following conjecture. Let E be an elliptic curve and suppose that the group of rational points $E(Q)$ has positive rank. Let a be a point of infinite order. Then they conjectured that the reduction of a mod (p) generates $E(F_p)$ for infinitely many primes p. This conjecture was proved in [3] for the case that E has complex multiplication, assuming the generalized Riemann hypothesis (GRH). The case when E has no complex multiplication is still open, even assuming the generalized Riemann hypothesis. As Serre observed in [6], if the conjecture of Lang and Trotter is true, then $E(F_p)$ is cyclic infinitely often. Indeed, assuming GRH, Serre showed that this was the case. In [5], the assumption of the GRH was removed in the case that E has complex multiplication (CM) by an order in an imaginary quadratic field. Thus, if E has CM, then $E(F_p)$ is cyclic infinitely often. The elimination of GRH from Serre's proof involved the use of sieve methods and an analogue of the Bombieri-Vinogradov theorem in algebraic number fields. Such an analogue is non-existent in the non-CM case and it is highly desirable to have one, for more than one reason. Moreover, sieve methods break down completely in the non-CM case.

In this paper, we will consider the following elliptic curves:

$$E_a: y^2 = (x^2 + 1)(x + a), \quad a \in Q.$$

*Research partially supported by NSERC grant A9418.

$$j_a = 54a^4 - 738a^2 + 27a + 27.$$

There are precisely thirteen values of the j-invariant, namely

$$j = 2^6 3^3, 2^6 5^3, 0, -3^3 5^3, -2^{15}, -2^{15} 3^3,$$
$$-2^{18} 3^3 5^3, -2^{15} 3^3 5^3 11^3, -2^{18} 3^3 5^3 23^3 29^3,$$
$$2^3 3^3 11^3, 2^4 3^3 5^3, 3^3 5^3 17^3, -3^1 2^{15} 5^3,$$

for which a given elliptic curve E over Q has complex multiplication. Thus, there are only finitely many values of a for which E_a has complex multiplication. Thus, for all but finitely many values of a, E_a has no complex multiplication.

Recently, Elkies [2] proved that any elliptic curve E defined over Q has infinitely many primes p for which E has supersingular reduction (mod p). We will utilise this fact together with Theorem 1 to deduce.

Theorem 2. *Let E be the elliptic curve E_a defined above. There are infinitely many primes p such that $E(F_p)$ is cyclic.*

In order to prove these theorems, we will need the following lemma which is of interest in its own right.

Lemma 1. Let $g: E_1 \to E_2$ and $f: E_1 \to E_3$ be morphisms of elliptic curves such that $\ker g \subseteq \ker f$. Then there is a morphism $h: E_2 \to E_3$ such that $f = g \circ h$.

Proof. Let s be a section of g and define $h(x) = f(s(x))$. This is independent of the choice of section. Indeed, if t is another section of g, then $f(s(x) - t(x)) = 0$ if and only if $s(x) - t(x)$ is in the kernel of f. But by definition, $s(x) - t(x)$ is in the kernel of g, which is contained in the kernel of f, by hypothesis. This shows that h is well-defined. h is clearly a morphism of elliptic curves.

Lemma 2. Let p and q be distinct prime numbers. Suppose that $p > 2$ and that E has good reduction (mod p). *Then p splits completely in $Q(E_q)$ if and only if $E(F_p)$ contains a subgroup of type (q, q).*

Proof. Let $\bar{E}$ denote the reduction of E over F_p and let π_p denote the Frobenius endomorphism of $\bar{E}$ over $\bar{F}_p$, given by $\pi_p(x) = x^p$. Then, the set of fixed points of

$$\pi_p: \bar{E} \to \bar{E}$$

constitute $E(F_p)$. Thus, $E(F_p)$ contains a subgroup of type (q, q) if and only if π_p acts trivially on the q-division points of $\bar{E}$, because the q-division points of $\bar{E}$ over $\bar{F}_p$ constitute a subgroup isomorphic to $Z/qZ \times Z/qZ$. We conclude that the decomposition group of any prime lying above p is trivial if and only if $E(F_p)$ contains a (q, q) group. This is the desired result.

COROLLARY.

Let $p > 2$. $E(F_p)$ is cyclic if and only if p does not split completely in all of the fields $Q(E_q)$ as q ranges over the primes.

Proof. $E(F_p)$ is cyclic if and only if it does not contain a (q, q) group for every prime p. For $q \neq p$, the result is immediate from the lemma. Suppose therefore that $q = p$ and that $E(F_p)$ contains a subgroup of type (p, p). Then $p^2 \leqslant p + 1 + 2\sqrt{p}$ by familiar estimates for the size of $E(F_p)$. But this last inequality forces $p = 2$.

We are now ready to prove Theorem 1.

Proof of Theorem 1. If $E(F_p)$ contains a subgroup of type (q, q) for some q, then this subgroup is contained in the set of fixed points of the Frobenius endomorphism π_p. If f_q denotes the endomorphism of multiplication by q, then

$$\ker f_q \subseteq \ker(\pi_p - 1).$$

By Lemma 1, we deduce that

$$(\pi_p - 1)/q$$

is an algebraic integer. If E has supersingular reduction (mod p), then $\pi_p = \pm\sqrt{-p}$. If $q > 2$, then

$$(\pm\sqrt{-p} - 1)/q$$

is never an algebraic integer. Therefore, $E(F_p)$ does not contain a subgroup of type (q, q) when $q > 2$. Thus, the 2-complement of $E(F_p)$ is cyclic.

If E is given in Weierstrass form:

$$y^2 = x^3 + ax + b,$$

and the roots of $x^3 + ax + b = 0$ are x_1, x_2, x_3, then the 2-division points are just the points $(x_i, 0), i = 1, 2, 3$ together with the point at infinity. If p is a prime for which E has supersingular reduction, then $E(F_p)$ has size $p + 1$. By Theorem 1, we know that the 2-complement is cyclic. If $E(F_p)$ contains the 2-division points, then by lemma 2, p splits completely in $Q(E_2)$, that is, the field obtained by adjoining x_1, x_2, x_3. For the curves E_a, we have that $Q(E_2) \supset Q(\sqrt{-1})$. Therefore if p splits completely in $Q(E_2)$, it splits completely in $Q(i)$ so that $p \equiv 1 (\text{mod } 4)$ is forced. Thus, 4 cannot divide $p + 1$ and so $E(F_p)$ is cyclic. This proves Theorem 2.

It is clear from the above discussion that the same argument shows that the curve

$$E: y^2 = x^3 + ax + b, \quad a, b \in Q$$

has the property that $E(F_p)$ is cyclic whenever E has supersingular reduction (mod p) and the roots of $x^3 + ax + b = 0$ generate $Q(i)$.

It is also interesting to note that for each of the curves E_a there is no prime $p \equiv 3$ (mod 4) for which E_a has supersingular reduction.

References

[1] Deuring M, Die typen der multiplikatorenringe elliptischer funktionenkörper, *Abh. Math. Sem. Hanisischen Univ.* **14** (1941) 191–272
[2] Elkies N, The existence of infinitely many supersingular primes for every elliptic curve over Q, *Invent. Math.* **89** (1987) 561–567
[3] Gupta R and Ram Murty M, Primitive points on elliptic curves, *Compos. Math.* **58** (1986) 13–44
[4] Lang S and Trotter H, Primitive points on elliptic curves, *Bull. Am. Math. Soc.* **83** (1977) 289–292
[5] Ram Murty M, On Artin's conjecture, *J. Number Theory* **16** (1983) 147–168
[6] Serre J-P, *Resumé de cours* (1977) (Oeavres: Springer Verlag) (1986)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 251–262.
© Printed in India.

The Manin–Drinfeld theorem and Ramanujan sums

V KUMAR MURTY[1,*] and DINAKAR RAMAKRISHNAN[2,**]

*Department of Mathematics, University of Toronto, Toronto, Ontario, Canada M5S 1A1

**Department of Mathematics, Duke University, Durham, NC 27706, USA and Cornell University, Ithaca, NY 14853, USA

Abstract. The Manin–Drinfeld theorem asserts the finiteness of the cuspidal divisor class group of a modular curve corresponding to a congruence subgroup. The purpose of the note is to draw attention to the connection between this theorem and Ramanujan sums, and to the question of what happens for non-congruence subgroups.

Keywords. Modular curve; cuspidal class group; Eisenstein series; Ramanujan sums; non-congruence subgroups.

1. Introduction

We consider the upper half plane

$$\mathscr{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$$

on which the group $GL_2^+(\mathbb{R})$ acts by fractional linear transformations. Let Γ denote a discrete subgroup of $SL_2(\mathbb{R})$ of (co-) finite volume, and consider the quotient

$$Y(\Gamma) = \Gamma \backslash \mathscr{H}.$$

We know that $Y(\Gamma)$ is an open Riemann surface which can be compactified by adding the finite set $\Gamma \backslash \mathbb{P}(\mathbb{R})$ of cusps. The resulting compact Riemann surface will be denoted $X = X(\Gamma)$. Viewing X as a smooth algebraic curve, and fixing a base point, we have an embedding $X \to J = J(X)$, the Jacobian of X. We are interested in the subgroup $C = C(\Gamma)$ of J spanned by the image of the cusps. If Γ is a congruence subgroup, the theorem of Manin and Drinfeld asserts that C is finite. The purpose of this paper is to draw attention to the connection between this theorem and Ramanujan sums, and to the question of what happens for general Γ.

The original arguments of Manin [8] and Drinfeld [3] use Hecke operators. For non-congruence subgroups, there does not yet exist a good theory of such operators, (cf. [1] for a discussion of the problems involved) and so this approach does not seem to generalize. Moreover, as observed by Rohrlich (see [6]), $C(\Gamma)$ is infinite for a general non-congruence subgroup Γ.

Another way of studying $C(\Gamma)$ is by observing the connection between cuspidal divisors of degree zero and differentials of the third kind. These differentials are

[1] Research partially supported by an NSERC grant.

[2] Alfred P Sloan Fellow. Research partially supported by the NSF.

given by Eisenstein series of weight 2 for Γ. The finiteness of $C(\Gamma)$ is then equivalent to the rationality of the periods of such (suitably normalized) differentials. This point of view is essentially the one taken by Schoeneberg [11] (see also Stevens [15] for a modern treatment). It was observed by Scholl [12] that the rationality of these periods is, in turn, equivalent to the algebraicity of the Fourier coefficients of the Eisenstein series. We review this in § 2.

When Γ is suitably normalized, the nth Fourier coefficient of the Eisenstein series can be written as a linear combination of sums of the form

$$(*) \qquad \pi^2 n \sum_{c>0} \frac{1}{c^2} \sum_{\substack{0 \leqslant d < c \\ \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right) \in \Gamma_\infty \backslash \Gamma}} \exp(2\pi i n d/c).$$

The inner sum may be thought of as a generalized Ramanujan sum. If Γ is a congruence subgroup, it can in fact be written in terms of (the usual) Ramanujan sums and evaluated explicitly. (Note that Ramanujan first introduced these sums in the very different context of the circle method.) This explicit evaluation allows us to sum the series in (*) and show that it lies in $\bar{\mathbb{Q}}$. We thus get what seems to be a slightly different proof of the Manin–Drinfeld theorem. The calculations are explained in § 3.

It is a very interesting question whether the classical evaluation of Ramanujan sums can be extended in any way to our generalized sums. We study this in one concrete case, namely that of the Fermat curve F_N given by

$$X^N + Y^N = 1.$$

Following Fricke and Klein [4], F_N can be written as $Y(\Gamma)$ with Γ a non-congruence subgroup of $\Gamma(2)$. We discuss this in § 4. We also raise a question about the Heisenberg curves which are cyclic covers of Fermat curves.

Finally, in § 5, we study the correspondence between the Fermat curve $\bar{F}_N$ and the modular curve $X(2N)$, considered by Kubert and Lang [6]. We view it as an algebraic cycle on the surface $\bar{F}_N \times X(2N)$ and show that, if $N > 7$ is prime, then this cycle is an element of finite order in the Néron–Severi group. It is intriguing to ask whether this has any direct connection with the finiteness of the cuspidal divisor class group on either curve.

2. Eisenstein series

Let X be a compact Riemann surface, and D a divisor of degree zero. Then, by the Riemann–Roch theorem, there is a differential ω of the third kind whose residual divisor $\operatorname{res}\omega$ is D. This ω can be made unique by specifying that its period with respect to any integral 1-cycle disjoint from D is purely imaginary. We shall denote this distinguished ω by ω_D. Then, we see that D is a torsion divisor if and only if the periods of ω_D lie in $2\pi i\mathbb{Q}$. Indeed, if $nD = (f)$, then we may take $\omega_D = \mathrm{d}f/nf$. Conversely, if ω_D has the stated property, then we can define the function

$$f(P) = \exp\left(\int_{\mathcal{O}}^{P} n\omega_D\right),$$

where $\mathcal{O}$ is a base point. It is easily seen that $(f) = nD$.

Now, suppose that $X = X(\Gamma)$ and that Γ is such that $Y(\Gamma)$ has a finite volume. In this case, the set of cusps is finite; let us write it as

$$S = \{\kappa_1, \ldots, \kappa_h\}.$$

We shall *assume* that ∞ is a cusp, say κ_1. To simplify the discussion still further, let us *assume* that $\Gamma \subseteq SL_2(\mathbb{Z})$. For each i, denote by Γ_i the stabilizer of κ_i in Γ. (We shall sometimes write Γ_∞ for Γ_1.) Let us fix an element σ_i in $SL_2(\mathbb{Z})$ so that $\sigma_i \infty = \kappa_i$. Then, there is a positive integer μ so that

$$\sigma_i^{-1}\Gamma_i\sigma_i = \left\{ \pm \begin{pmatrix} 1 & \mu m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}.$$

For $z = x + iy$, we set (following Hecke)

$$G_i(z) = \lim_{s \to 1} s y^{s-1} \sum_{\substack{\sigma \in \Gamma_i \backslash \Gamma \\ \sigma = \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right)}} (cz + d)^{-2} |cz + d|^{2-2s}.$$

Then, G_i is a real-analytic Eisenstein series of weight 2. Moreover, if $D = \sum m_i \kappa_i$ is a divisor of degree zero, let us set

$$G_D(z) = \sum m_i G_i(z).$$

It is known (see [12], Prop. 2]) that

$$\omega_D = 2\pi i G_D(z) dz.$$

Moreover, there is the following connection between the order of D and the Fourier expansion of G_D at ∞.

PROPOSITION [12]

The following are equivalent:

(a) *D is of finite order in J*
(b) *All the Fourier coefficients of G_D at ∞ are algebraic numbers.*

Following the treatment in Kubota [7], we find that

$$G_j(z) = \delta_j - \pi y C - 4\pi^2 \sum_{m=1}^{\infty} m A_{j,m} \exp(2\pi i m z)$$

where

$$\delta_j = \begin{cases} 1 & \text{if } j = 1 \\ 0 & \text{if } j \neq 1, \end{cases}$$

C is a constant (independent of j) and

$$A_{j,m} = \lim_{s \to 1+} \sum_{c > 0} \frac{1}{c^{2s}} \left(\sum_{\substack{0 \leq d < \mu c \\ \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right) \in \sigma_j^{-1}\Gamma}} \exp(2\pi i m d / c\mu) \right).$$

An immediate consequence of the above Proposition is the following.

PROPOSITION

The following are equivalent:

(a) $C(\Gamma)$ *is finite*
(b) *For each* $1 \leqslant j \leqslant h$, *and* $m \geqslant 1, \pi^2(A_{j,m} - A_{1,m}) \in \bar{\mathbb{Q}}$.

3. Congruence subgroups

If Γ is a congruence subgroup, the series $A_{j,m}$ can be evaluated explicitly. One immediately reduces to the case that $\Gamma = \Gamma(N)\{\pm I\}$ where $\Gamma(N)$ is the principal congruence subgroup of level N. We shall perform the calculation for the cusps $\kappa_1 = \infty$ and $\kappa_2 = 0$, the general case being similar. We have $\sigma_1 = I$ and $\sigma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\mu = N$. We see that

$$\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma \Leftrightarrow c \equiv 0 \,(\mathrm{mod}\, N), \quad d \equiv \pm 1 \,(\mathrm{mod}\, N), \quad (c,d) = 1$$

$$\begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \sigma_2^{-1}\Gamma \Leftrightarrow c \equiv \pm 1 \,(\mathrm{mod}\, N), \quad d \equiv 0 \,(\mathrm{mod}\, N), \quad (c,d) = 1.$$

Hence,†

$$A_{1,m} = \sum_{\substack{c>0 \\ c \equiv 0 (\mathrm{mod}\, N)}} \frac{1}{c^2} \left(\sum_{\substack{0 \leqslant d < Nc \\ d \equiv \pm 1 (\mathrm{mod}\, N) \\ (d,c)=1}} \exp(2\pi i m d/cN) \right)$$

and

$$A_{2,m} = \sum_{\substack{c>0 \\ c \equiv \pm 1 (\mathrm{mod}\, N)}} \frac{1}{c^2} \left(\sum_{\substack{0 \leqslant d < Nc \\ (d,c)=1 \\ d \equiv 0 (\mathrm{mod}\, N)}} \exp(2\pi i m d/cN) \right).$$

We use the Ramanujan sum

$$\sum_{\substack{0 \leqslant h < k \\ (h,k)=1}} \exp(2\pi i m h/k) = \sum_{j \mid (m,k)} \mu(k/j)\, j,$$

where $\mu(x)$ denotes the Mobius function. We find that

$$A_{2,m} = \sum_{\substack{j \mid m \\ (j,N)=1}} \frac{1}{j} \sum_{c_0 \equiv \pm \bar{j} (\mathrm{mod}\, N)} \frac{\mu(c_0)}{{c_0}^2}$$

where $\bar{j}$ denotes the inverse of j (mod N). We can simplify this further:

$$A_{2,m} = \frac{1}{\phi(N)} \sum_{\substack{j \mid m \\ (j,N)=1}} \frac{1}{j} \sum_{\chi} (\chi(j) + \chi(-j)) \frac{1}{L(2,\chi)}$$

$$= \frac{2}{\phi(N)} \sum_{\substack{j \mid m \\ (j,N)=1}} \frac{1}{j} \sum_{\chi(-1)=1} \frac{\chi(j)}{L(2,\chi)}$$

†To be precise, we should really write $A_{1,m}$ and $A_{2,m}$ as limits as $s \to 1^+$. However, the discussion in this section justifies setting $s = 1$.

where the inner sum is over even Dirichlet characters (mod N). It follows that $\pi^2 A_{2,m} \in \bar{\mathbb{Q}}$. To evaluate $A_{1,m}$, we observe that if $\varepsilon = \pm 1$, then,

$$\sum_{\substack{0 \leqslant d < Nc \\ d \equiv a (\mathrm{mod}\, N) \\ (d,c)=1}} \exp(2\pi i m d/cN) = \sum_{\substack{0 \leqslant d < Nc \\ d \equiv a (\mathrm{mod}\, N)}} \exp(2\pi i m d/cN) \sum_{j \mid (d,c)} \mu(j)$$

$$= \sum_{\substack{j \mid c \\ (j,N)=1}} \mu(j) \sum_{\substack{0 \leqslant d_0 < Nc/j \\ d_0 \equiv \bar{ej} (\mathrm{mod}\, N)}} \exp(2\pi i m j d_0/cN)$$

where, we have written $d = jd_0$ and $\bar{j}$ for the inverse of $j (\mathrm{mod}\, N)$. If we further write $d_0 = \varepsilon\bar{j} + d_1 N$, the sum becomes

$$\sum_{\substack{j \mid c \\ (j,N)=1}} \mu(j) \sum_{0 \leqslant d_1 < (c/j)} \exp[2\pi i m j(\varepsilon j + d_1 N)/cN]$$

$$= \sum_{\substack{j \mid c \\ (j,N)=1}} \mu(j) \exp(2\pi i m \varepsilon j \bar{j}/cN) \sum_{0 \leqslant d_1 < (c/j)} \exp[2\pi i m d_1/(c/j)].$$

Let us write $c = jc_0$. The inner sum is 0 unless $m \equiv 0 (c_0)$ in which case it is c/j. Thus, we find the above equal to

$$c \sum_{\substack{j \mid c \\ (j,N)=1 \\ m \equiv 0 (\mathrm{mod}\, c/j)}} \frac{\mu(j)}{j} \exp(2\pi i m \varepsilon j \bar{j}/cN).$$

Substituting this into the series for $A_{1,m}$, and rearranging, we find that

$$A_{1,m} = \sum_{\varepsilon = \pm 1} \sum_{\substack{c_0 \mid m \\ c_0 \equiv 0 (\mathrm{mod}\, N) \\ c_0 > 0}} \frac{1}{c_0} \sum_{\substack{j > 0 \\ (j,N)=1}} \frac{\mu(j)}{j^2} \exp(2\pi i \varepsilon m \bar{j}/c_0 N)$$

$$= \sum_{\varepsilon = \pm 1} \sum_{\substack{N \mid c_0 \mid m \\ c_0 > 0}} \frac{1}{c_0} \sum_{\substack{1 \leqslant a < N \\ (a,N)=1}} \exp(2\pi i \varepsilon m \bar{u}/c_0 N) \sum_{\substack{j \equiv a (\mathrm{mod}\, N) \\ j > 0}} \frac{\mu(j)}{j^2}.$$

The innermost sum is written in terms of Dirichlet L-series as before:

$$A_{1,m} = \sum_{\varepsilon} \sum_{c_0} \sum_{u} \frac{1}{c_0} \exp(2\pi i^* \bar{u}) \frac{1}{\phi(N)} \sum_{\chi} \chi(a) \frac{1}{L(2,\chi)}$$

where we have written * for $\varepsilon M/c_0 N$. Rearranging the sums, and observing that

$$\sum_{a} \exp(-2\pi i^* \bar{a}) \bar{\chi}(a) = \chi(-1) \sum_{a} \exp(2\pi i^* \bar{a}) \bar{x}(a),$$

we deduce that

$$A_{1,m} = \frac{2}{\phi(N)} \sum_{\substack{N \mid c_0 \mid m \\ c_0 > 0}} \frac{1}{c_0} \sum_{\substack{1 \leqslant a < N \\ (a,N)=1}} \exp(2\pi i m \bar{a}/c_0 N) \sum_{\chi(-1)=1} \frac{\bar{\chi}(a)}{L(2,\chi)}.$$

Hence, $\pi^2 A_{1,m} \in \bar{\mathbb{Q}}$ also. This, therefore, proves that (∞)–(0) is a point of finite order in the Jacobian of $X(\Gamma)$.

4. Fermat curves and Heisenberg curves

We define the Fermat curve F_N of degree N by

$$X^N + Y^N = 1.$$

There is a natural smooth compactification $\bar{F}_N$ of F_N in $\mathbb{P}^2$. Following Fricke and Klein (cf. Rohrlich [10]), we know that it is possible to write F_N as a modular curve corresponding (in general) to a non-congruence subgroup. We begin by reviewing this parametrization.

For any $\tau \in \mathscr{H}$, let $L_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$ and

$$p_\tau(z) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L_\tau} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

the corresponding Weierstrass function. Let

$$w_k = \begin{cases} 1 & \text{if } k = 1 \\ \tau + 1 & \text{if } k = 2 \\ \tau & \text{if } k = 3 \end{cases}$$

and set $e_k = p_\tau(\frac{1}{2}w_k)$. Note that $\{0, \frac{1}{2}, \frac{1}{2}\tau, \frac{1}{2}(\tau+1)\}$ represent the points of order 2 on the elliptic curve $\mathbb{C}/L_\tau$. In particular, the e_k are distinct. We define the function

$$\lambda(\tau) = (e_2 - e_3)/(e_1 - e_3).$$

This function is analytic and non-zero on $\mathscr{H}$. We have the following facts regarding λ:

(a) λ is an automorphic function for $\Gamma(2)$
(b) λ maps H onto $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$
(c) λ takes the values $0, 1, \infty$ at $\infty, 0, 1$ respectively.

Because of (a), λ defines a function on the open Riemann surface $Y(2) = \Gamma(2)\backslash\mathscr{H}$. Moreover, we may identify

$$Y(2) \to F_1$$

by $z \to (\lambda(z), 1 - \lambda(z))$. Now, F_N can be described as a finite ramified cover of $F_1 = Y(2)$. In any simply connected open subset U of $\mathbb{P}^1 - \{0, 1, \infty\}$, we can find a well-defined N-th root $\tilde{x}$ of λ and $\tilde{y}$ of $1 - \lambda$. We can extend $(\tilde{x}, \tilde{y})$ as a pair of multi-valued functions on $\mathbb{P}^1 - \{0, 1, \infty\}$. The covering space on which $(\tilde{x}, \tilde{y})$ become single-valued is the affine curve F_N given by

$$\tilde{x}^N + \tilde{y}^N = 1.$$

The monodromy of $\tilde{x}$ and $\tilde{y}$ can be described in a simple way. Take $\gamma \in \Gamma(2) = \pi_1(\mathbb{P}^1 - \{0, 1, \infty\})$. Then, there are integers $s(\gamma)$ and $t(\gamma)$ such that

$$^{\gamma}\log \lambda = \log \lambda + 2\pi i s(\gamma)$$

$$^{\gamma}\log(1 - \lambda) = \log(1 - \lambda) + 2\pi i t(\gamma).$$

It follows that $\pi_1(F_N) = \Gamma$ where

$$\Gamma = \{\gamma \in \Gamma(2): s(\gamma) \equiv t(\gamma) \equiv 0 (\mathrm{mod}\, N)\}.$$

In other words, Γ is the kernel of the map

$$\Gamma(2) \to \mathbb{Z}/N \times \mathbb{Z}/N$$

$$\gamma \to (s(\gamma) \bmod N,\ t(\gamma) \bmod N).$$

There is yet another way to view Γ. We note that $\Gamma(2)$ is a free group on the generators $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. These two generators correspond to the positively oriented cycles around 0 and 1 in $\mathbb{P}^1 - \{0, 1, \infty\}$. The reduction mod N of the abelianization map gives:

$$\Gamma(2) \to \mathbb{Z}/N \times \mathbb{Z}/N$$

which coincides with the map of the previous paragraph. It follows easily from this description that in general Γ is a non-congruence subgroup.

It is also possible to describe $s(\gamma)$, $t(\gamma)$ explicitly in terms of Dedekind sums. The key idea is to relate λ to the Dedekind η function and use the well-known transformation formulae for $\log \eta$. We begin by recalling the latter result (see, for example, Siegel [14]).

PROPOSITION

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be in* $SL_2(\mathbb{Z})$. *Then*

$$\log \eta(\gamma z) - \log \eta(z) = \begin{cases} \pi i b/12 & \text{if } c = 0 \\ \frac{1}{2} \log(-i(cz + d)) + \pi i \dfrac{a + d}{12c} - \pi i D(d, c) & \text{if } c > 0. \end{cases}$$

Here,

$$D(d, c) = \sum_{0 \leqslant j < c} ((j/c))((jd/c))$$

is the Dedekind sum and

$$((x)) = \begin{cases} x - [x] - \frac{1}{2} & \text{if } x \notin \mathbb{Z} \\ 0 & \text{otherwise.} \end{cases}$$

Next, we relate λ to the η function.

Lemma. We have

$$\lambda(z) = 16 \exp(\pi i/3)(\eta(2z)/\eta(\tfrac{1}{2}(z + 1)))^8,$$

$$1 - \lambda(z) = \exp(\pi i/3)(\eta(\tfrac{1}{2}z)/\eta(\tfrac{1}{2}(z + 1)))^8.$$

Proof. Let us set $q_2 = \exp(\pi i z)$. From Fricke and Klein [4] we know that

$$\lambda(z) = 16 q_2 \prod_{n=1}^{\infty} (1 + {q_2}^{2n})^8 (1 + {q_2}^{2n-1})^{-8},$$

$$1 - \lambda(z) = \prod_{n=1}^{\infty} (1 - {q_2}^{2n-1})^8 (1 + {q_2}^{2n-1})^{-8}.$$

The result follows easily from these.

Using this lemma, we may define $\log\lambda$ and $\log(1-\lambda)$ in terms of $\log\eta$ and study their transformation properties.

PROPOSITION

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$. *Then*

$$s(\gamma) = \begin{cases} b/2 & \text{if } c = 0 \\ \dfrac{a+d}{2c} - 4\left[D\left(d, \dfrac{c}{2}\right) - D(d-c, 2c) \right] & \text{if } c > 0, \end{cases}$$

$$t(\gamma) = \begin{cases} 0 & \text{if } c = 0 \\ 4[D(d-c, 2c) - D(d, 2c)] & \text{if } c > 0. \end{cases}$$

Proof. From the previous lemma, we have

$$\log\lambda(z) = \log(16\exp(\pi i/3)) + 8\log\eta(2z) - 8\log\eta(\tfrac{1}{2}(z+1)).$$

Suppose that $c > 0$. Since

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 2b \\ c/2 & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

we have

$$\log\eta\left(\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\gamma z\right) - \log\eta\left(\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} z\right)$$

$$= \frac{1}{2}\log(-i(cz+d)) + \pi i\left(\frac{a+d}{6c}\right) - \pi i D\left(d, \frac{c}{2}\right).$$

Similarly,

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1/2 \\ 0 & 1/2 \end{pmatrix} = \begin{pmatrix} a+c & \frac{1}{2}(b+d-a-c) \\ 2c & d-c \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Hence,

$$(**) \qquad \log\eta\left(\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}\gamma z\right) - \log\eta\left(\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} z\right)$$

$$= \tfrac{1}{2}\log(-i((cz+d))) + \pi i\left(\frac{a+d}{24c}\right) - \pi i D(d-c, 2c).$$

Thus,

$$\frac{1}{8}((\log\lambda)(\gamma z)-(\log\lambda)(z))$$

$$=\left[\pi i\left(\frac{a+d}{6c}\right)-\pi iD\left(d,\frac{c}{2}\right)\right]-\left[\pi i\left(\frac{a+d}{24c}\right)-\pi iD(d-c,2c)\right]$$

and so

$$s(\gamma)=\frac{a+d}{2c}+4\left[D(d-c,2c)-D\left(d,\frac{c}{2}\right)\right].$$

If $c=0$, a similar calculation gives

$$\frac{1}{8}((\log\lambda)(\gamma z)-(\log\lambda)(z))=\pi i\left(\frac{2b}{12}\right)-\frac{\pi i(b+d-a-c)}{24}=\frac{\pi ib}{8},$$

and so $s(\gamma)=b/2$. For $t(\gamma)$, we repeat the above using the relation

$$\log(1-\lambda)(z)=\frac{\pi i}{3}+8(\log\eta(\tfrac{1}{2}z)-\log\eta(\tfrac{1}{2}(z+1)))$$

given by the lemma. Since

$$\begin{pmatrix}1&0\\0&2\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&1/2\end{pmatrix}=\begin{pmatrix}a&b/2\\2c&d\end{pmatrix}$$

we have, for $c>0$,

$$\log\eta(\tfrac{1}{2}\gamma z)-\log\eta(\tfrac{1}{2}z)=\frac{1}{2}\log(-i(cz+d))+\pi i\left(\frac{a+d}{24c}\right)-\pi iD(d,2c).$$

Combining this with (**), we find that

$$2\pi it(\gamma)=8\left[\left(\pi i\frac{a+d}{24c}-\pi iD(d,2c)\right)-\left(\pi i\frac{a+d}{24c}-\pi iD(d-c,2c)\right)\right]$$

and so

$$t(\gamma)=4[D(d-c,2c)-D(d,2c)]$$

if $c>0$. If $c=0$, we have

$$2\pi it(\gamma)=8\left[\frac{\pi ib}{24}-\frac{\pi ib}{24}\right]=0.$$

It is interesting to ask whether the expressions for $s(\gamma)$ and $t(\gamma)$ given by this Proposition can be used to evaluate the generalized Ramanujan sums corresponding to our group Γ, a typical one of which is

$$\sum_{\substack{0\leqslant d<2Nc\\ \left(\begin{smallmatrix}*&*\\c&d\end{smallmatrix}\right)\in\Gamma_\infty\backslash\Gamma}}\exp(2\pi imd/2Nc).$$

$$\sum_{\substack{0\leqslant d<2Nc \\ \gcd\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right)=0 \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\equiv 0 \pmod N}} \exp(2\pi i m d/2N).$$

On the other hand, Rohrlich [10] has shown that the group $C(\Gamma)$ *is* finite. Therefore, invoking the Proposition at the end of § 2, we get the following curious result.

PROPOSITION

For all $m \geqslant 1$,

$$\lim_{s\to 1+} \pi^2 \sum_{c>0} \frac{1}{c^{2s}} \left\{ \sum_{\substack{0\leqslant d<2Nc \\ \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right)\in \Gamma_\infty\backslash\Gamma}} \exp(2\pi i m d/2Nc) - \sum_{\substack{0\leqslant d<2Nc \\ \left(\begin{smallmatrix} c & d \\ * & * \end{smallmatrix}\right)\in \Gamma_\infty\backslash\Gamma}} \exp(2\pi i m d/2Nc) \right\} \in \bar{\mathbb{Q}}.$$

Indeed this is equivalent to the fact that $(\infty)-(0)$ *is torsion.*

Next, we turn our attention to another class of curves. For any ring R, the R-points of the Heisenberg group are defined to be

$$H_R = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in R \right\}.$$

There is a natural homomorphism

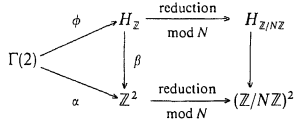
$$\phi: \Gamma(2) \to H_{\mathbb{Z}}$$

given on the generators by

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

For every integer $N \geqslant 1$, we have a (commutative) diagram:



where α and β are the abelianization maps. (In particular, β tends

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

to the pair (a, b)). Let ϕ_N denote the composition of ϕ with reduction mod N. The *Heisenberg curve* H_N is $\Gamma\backslash\mathscr{H}$ where $\Gamma = \ker\phi_N$. The compactification $\bar{H}_N$ of H_N is a cover of $\mathbb{P}^1$ ramified only over $\{0, 1, \infty\}$. It is a fact (due to Deligne) that $\bar{H}_N$ can be defined over $\mathbb{Q}$.

It is known (see [9]) that ϕ can be defined by means of the monodromy of the dilogarithm function

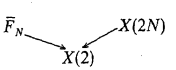
$$\ell_2(z) = -\int_0^z \log(1-t)\frac{\mathrm{d}t}{t}.$$

(More precisely, one considers the monodromy of $\ell_2(z)$, $\log z$ and $\log(1-z)$.) As in the case of the Fermat curves, we can write a formula for the Fourier coefficients of the Eisenstein series of weight 2 for $\ker\phi_N$, in terms of certain generalized Ramanujan sums. It will be a very interesting problem to determine the arithmetic nature of these coefficients and the structure of the cuspidal class group $C(\ker\phi_N)$.

Both in the case of $\bar{F}_N$ and $\bar{H}_N$, we have curves expressed as covers of $\mathbb{P}^1$ ramified only at $\{0, 1, \infty\}$. There is a general result of Belyi [2] that a smooth projective curve has a model over $\bar{\mathbb{Q}}$ if and only if it can be written as a cover of $\mathbb{P}^1$ ramified only at $\{0, 1, \infty\}$. A natural question to ask is the following. Given the cover $X \to \mathbb{P}^1$ ramified only at $\{0, 1, \infty\}$, what further hypotheses are needed to ensure that the inverse image of $\{0, 1, \infty\}$ give points of finite order in the Jacobian of X? (We know that *some* further hypotheses will be necessary since the proof of Belyi shows that *any* finite set of algebraic points can be made to lie over $\{0, 1, \infty\}$.)

5. The Kubert–Lang correspondence

In this section, we discuss a matter related to the parametrization of the Fermat curve which was discussed in the previous section. Using the λ-function, we have seen that it is possible to exhibit $\bar{F}_N$ as a cover of $X(2) = \mathbb{P}^1$ corresponding to a subgroup Γ of $\Gamma(2)$. This cover is ramified only over $\{0, 1, \infty\}$ and is in fact totally ramified at these points. We also have the modular curve $X(2N)$ as a cover of $X(2)$ and, as observed by Kubert and Lang, this cover has the same ramification properties. Therefore we have a diagram



where the arrows are given by rational finite maps. Thus we get an unramified correspondence from $\bar{F}_N$ to $X(2N)$. Kubert and Lang [6, p.196] use this to show that if F_N has infinitely many rational points in a number field k, then $X(2N)$ has infinitely many rational points in a finite extension of k, and conversely.

The correspondence gives, in a natural way, a divisor on the product $\bar{F} \times X(2N)$. It is interesting to consider the algebraic equivalence class of this divisor, D_N say. We have the following result.

PROPOSITION

Let N be a prime larger than 7. Then D_N is torsion in the Neron–Severi group $NS(\bar{F}_N \times X(2N))/(NS(\bar{F}_N) \oplus NS(X(2N)))$.

Proof. This follows easily from known properties of the Jacobians of Fermat and modular curves. Indeed, D_N gives rise to an endomorphism

$$(***) \qquad \mathrm{Jac}(\bar{F}_N) \to \mathrm{Jac}(X(2N)).$$

Let us recall the decomposition of $\mathrm{Jac}(\bar{F}_N)$ into simple factors. We have

$$\mathrm{Jac}(\bar{F}_N) \approx \prod_{i=1}^{N-2} A_i,$$

where each A_i is an abelian variety of dimension $\frac{1}{2}(N-1)$ and having complex multiplication (CM) by $\mathbb{Q}(\zeta_N)$. From the tables of Koblitz [5], we know that if $N > 7$ is prime, then over $\bar{\mathbb{Q}}$, A_i is isogenous to a power of an absolutely simple abelian variety of dimension > 1. On the other hand, it is a well known result of Shimura that

$$\mathrm{Jac}(X(2N)) \approx \prod A_f,$$

where the product ranges over certain cusp forms of weight 2 and, if A_f is of CM type, there is a splitting over $\bar{\mathbb{Q}}$: $A_f \approx E^n$ where E is an elliptic curve with CM and $n \geqslant 1$ ([13]). Thus, tensoring the homomorphism (***) with $\mathbb{Q}$ and observing that CM factors must map to CM factors, we conclude the result of the Proposition.

References

[1] Atkin A O L and Swinnerton-Dyer H P F, Modular forms on non-congruence subgroups, *Combinatorics, Proc. Symp. Pure Math. Am Math. Soc.* **19** (1968) 1–25

[2] Belyi G V, Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk USSR Ser. Mat. (Russian)* **43** (1979) 267–276

[3] Drinfeld V G, Two theorems on modular curves, *Funkc. Anal. i. Prilozen (Russian)* **7** (1973) 83–84

[4] Fricke R and Klein F, *Vorlesungen uber die theorie der elliptischen modulfunktionen* (New York: Johnson Reprint Corpn.) Vol. 2 (1966) (from the 1890 edition)

[5] Koblitz N, Gamma function identities and elliptic differentials on Fermat curves, *Duke Math. J.* **45** (1978) 87–99

[6] Kubert D and Lang S, *Modular units* Grundleheren der Math. Wissenschaften (Springer-Verlag) (1981)

[7] Kubota T, *Elementary theory of Eisenstein series* (Wiley) (1973)

[8] Manin J, Parabolic points and zeta functions of modular curves, *Izv. Akad. Nauk USSR Ser. Math. (Russian)* **36** (1972) 19–64

[9] Ramakrishnan D, A regulator for curves via the Heisenberg group, *Bull. Am. Math. Soc.* **5** (1981) 191–195

[10] Rohrlich D, Points at infinity on the Fermat curves, *Invent. Math.* **39** (1977) 95–127

[11] Schoeneberg B, *Elliptic modular functions, an introduction* (English translation from German) (Grundleheren: Springer-Verlag) (1974)

[12] Scholl A J, Fourier coefficients of Eisenstein series on non-congruence subgroups, *Math. Proc. Cambridge Philos. Soc.* **99** (1986) 11–17

[13] Shimura G, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, *Nagoya Math. J.* **43** (1971) 199–208

[14] Siegel C L, *Advanced analytic number theory* (Lecture Notes) (Bombay: Tata Institute of Fundamental Research) 2nd ed. (1980)

[15] Stevens G, *Arithmetic of modular curves, Progress in Mathematics* (Boston: Birkhauser) (1982)

© Printed in India.

On Ramanujan's modular identities

S RAGHAVAN
School of Mathematics, Tata Institute of Fundamental Research, Bombay 400 005, India

Abstract. For Ramanujan's modular identities connected with his well-known partition congruences for the moduli 5 or 7, we had given, in an earlier paper, natural and uniform proofs through the medium of modular forms. Analogous (modular) identities corresponding to the (more difficult) case of the modulus 11 are provided here, with the consequent partition congruences; the relationship with relevant results of N J Fine is also sketched.

Keywords. Ramanujan's modular identities; partition congruences; modular forms.

1. Introduction

For the partition function $p(\cdot)$, Ramanujan exhibited several interesting congruence relations and in particular, $p(5n+4) \equiv 0 \pmod 5$ for $n = 0, 1, 2, \ldots$ etc. Besides a simple proof for the above congruences modulo 5 via the modular equation of degree 5, Ramanujan gave an elegant proof in ([7], p. 5). First, he writes down the beautiful identity

$$x\frac{\prod_{n=1}^{\infty}(1-x^{5n})^5}{\prod_{n=1}^{\infty}(1-x^n)} = \sum_{n=0}^{\infty}\left\{\frac{x^{5n+1}}{(1-x^{5n+1})^2} - \frac{x^{5n+2}}{(1-x^{5n+2})^2} - \frac{x^{5n+3}}{(1-x^{5n+3})^2} + \frac{x^{5n+4}}{(1-x^{5n+4})^2}\right\} \tag{1}$$

and then, for the "allied function" $\prod_{n=1}^{\infty}\{(1-x^n)^5/(1-x^{5n})\}$, the identity

$$\frac{\prod_{n=1}^{\infty}(1-x^n)^5}{\prod_{n=1}^{\infty}(1-x^{5n})} = 1 - 5\left(\frac{x}{1-x} - \frac{2x^2}{1-x^2} - \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{6x^6}{1-x^6} - \frac{7x^7}{1-x^7} - \cdots\right) \tag{2}$$

To derive the above partition congruences modulo 5, Ramanujan applies to both sides of (1) an "averaging operator" U_5 which turns out essentially to be the operator T_5^5 considered by Hecke ([4], p. 839). In connection with the partition congruences

above modulo 7, Ramanujan wrote down the identity

$$x\prod_{n=1}^{\infty}(1-x^n)^3\prod_{n=1}^{\infty}(1-x^{7n})^3+8x^2\frac{\prod_{n=1}^{\infty}(1-x^{7n})^7}{\prod_{n=1}^{\infty}(1-x^n)}$$

$$=\sum_{n=0}^{\infty}\left\{\frac{x^{7n+1}(1+x^{7n+1})}{(1-x^{7n+1})^3}+\frac{x^{7n+2}(1+x^{7n+2})}{(1-x^{7n+2})^3}+\frac{x^{7n+4}(1+x^{7n+4})}{(1-x^{7n+4})^3}\right.$$

$$\left.-\frac{x^{7n+3}(1+x^{7n+3})}{(1-x^{7n+3})^3}-\frac{x^{7n+5}(1+x^{7n+5})}{(1-x^{7n+5})^3}-\frac{x^{7n+6}(1+x^{7n+6})}{(1-x^{7n+6})^3}\right\}. \tag{3}$$

He also gave an 'allied' identity

$$49x\prod_{n=1}^{\infty}(1-x^n)^3\prod_{n=1}^{\infty}(1-x^{7n})^3+8\frac{\prod_{n=1}^{\infty}(1-x^n)^7}{\prod_{n=1}^{\infty}(1-x^{7n})}$$

$$=8-7\left(\frac{x}{1-x}+\frac{4x^2}{1-x^2}-\frac{9x^3}{1-x^3}+\frac{16x^4}{1-x^4}-\frac{25x^5}{1-x^5}-\frac{36x^6}{1-x^6}+\frac{64x^8}{1-x^8}+\cdots\right). \tag{4}$$

For identities (1) and (2), there exist proofs due to Bailey ([1], [2]) and we were not able to find any proof for (3) in the literature at the time of writing [6] wherein we had provided a uniform (and what appeared to us as quite a natural) proof for all the identities (1)–(4) through the medium of modular forms of Haupttypus $(-2, 5, 1)$ and Nebentypus $(-3, 7, \varepsilon)$ in the sense of Hecke [4]. We had also indicated at the end of [6] the existence of identities such as (1)–(4) corresponding to the case of modulus 11 in connection with Ramanujan's partition congruences modulo 11. The object of this note is precisely to provide such identities.

It has been pointed out to us kindly by Professor N J Fine in a recent letter (subsequent to the Ramanujan Centenary Conference at Urbana-Champaign) that both the identities (3) and (4) had already been proved by him in [3] using identities involving elliptic functions, "without much difficulty". One finds in [3] also the identity

$$\sum_{0}^{\infty}p(11m+6)x^{m+1}=11x^5\frac{\prod_{n=1}^{\infty}(1-x^{11n})^{11}}{\prod_{n=1}^{\infty}(1-x^n)^{12}}(11^3+8.11\alpha+\alpha^2+11\beta) \tag{5}$$

stemming from "lengthy" calculations, where α, β are modular functions for the congruence subgroup $\Gamma_0(11)$ with integral coefficients in their Fourier expansions. In the sequel, we shall exhibit an identity involving $\sum_0^\infty p(11m+6)x^{m+1}$ and modular forms of Nebentypus $(-3, 11, \varepsilon)$; this will turn out to be the same as (5) after proper identification of α, β above with ratios of modular forms of Nebentypus $(-3, 11, \varepsilon)$. An "allied' identity involving

$$\prod_{n=1}^{\infty}(1-x^n)^{11}\Big/\prod_{n=1}^{\infty}(1-x^{11n})\quad\text{in lieu of}\quad x^5\prod_{n=1}^{\infty}(1-x^{11n})^{11}\Big/\prod_{n=1}^{\infty}(1-x^n)$$

is also derived later and this gives rise to a classical congruence $p_{11}(11n) \equiv p_1(n) \pmod{11}$ for $n = 1, 2, \ldots$, where $p_r(n)$ is the coefficient of x^n in $\prod_{n=1}^{\infty}(1-x^n)^r$.

We are convinced more than ever that an approach to the partition congruences modulo 5, 7 or 11 through modular forms is not only natural but also has an unmistakable simplicity of its own. For example, identities (4.14), (4.16), (4.17), (4.12) in [3] are transparent linear relations between modular forms of Nebentypus $(-3, 7, \varepsilon)$; the arguments in this context used in [3], appear, on the other hand, to be more involved.

2. Notation and preliminaries

A modular form of Nebentypus $(-k, p, \varepsilon)$ in the notation of Hecke ([4], p. 809) is a holomorphic function f of a complex variable z in the upper half-plane H such that for every $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$ with $c \equiv 0 \pmod{p}$, $f((az+b)(cz+d)^{-1}) = \varepsilon(d)\,(cz+d)^k f(z)$ for a character ε on $(\mathbb{Z}/p\mathbb{Z})^\times$ and further such that $f((qz+r)(sz+t)^{-1})(sz+t)^{-k}$ is bounded at infinity for every $\begin{pmatrix} q & r \\ s & t \end{pmatrix}$ in $SL_2(\mathbb{Z})$. The latter condition is equivalent to saying that f is bounded in a fundamental domain for the congruence subgroup $\Gamma_0(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod{p} \right\}$ in H. For prime p, $\Gamma_0(p)$ has exactly two cusps, namely at 0, ∞. We know from Hecke again that for $p = 11$ in particular and odd $k \geqslant 1$, the Eisenstein series

$$E_{1,k}(z) := \sum_{n=1}^{\infty} \left(\sum_{1 \leqslant d \mid n} d^{k-1} \left(\frac{n/d}{11} \right) \right) \exp(2\pi i n z),$$

$$E_{2,k}(z) := \gamma_k + \sum_{n=1}^{\infty} \left(\sum_{1 \leqslant d \mid n} d^{k-1} \left(\frac{d}{11} \right) \right) \exp(2\pi i n z)$$

with a well-defined rational number γ_k (e.g. $\gamma_3 = -3$, $\gamma_5 = 1275/11$) are of Nebentypus $(-k, 11, \varepsilon)$ with $\varepsilon(r) := (r/11)$, the Legendre symbol, while the "theta series with Grossencharacter"

$$\vartheta_k(z) := \sum_{\mu \in \mathbb{Z} + \mathbb{Z}\omega} \mu^{k-1} \exp(2\pi i z \mu\bar{\mu}) \quad (\text{with } \omega := \tfrac{1}{2} + \sqrt{-11})$$

is a cusp form of Nebentypus $(-k, 11, \varepsilon)$ for odd $k \geqslant 1$. Let $\eta(z)$ be Dedekind's function defined by

$$\eta(z) := \exp(2\pi i z/24) \prod_{n=1}^{\infty} (1 - \exp(2\pi i n z))$$

and $\eta_N(z) := \eta(Nz)$ for every integer $N \geqslant 1$. We know, from Hecke, that $\eta^2\eta_{11}^2$ is a modular form of Haupttypus $(-2, 11, 1)$. For $k = 3$, the three modular forms $E_{1,3}$, $E_{2,3}, \vartheta_3$ form a basis for the space of modular forms of Nebentypus $(-3, 11, \varepsilon)$. Further a basis for modular forms of Nebentypus $(-5, 11, \varepsilon)$ is provided by $E_{1,5}, E_{2,5}$, $\eta^2\eta_{11}^2 E_{1,3}, \eta^2\eta_{11}^2 E_{2,3}$ and $\eta^2\eta_{11}^2 \vartheta_3$, as may be easily verified. One may find in Hecke ([4], pp. 827, 828) tables for the constants term γ_k of the Eisenstein series above or

for the dimensions of the spaces of modular forms of Haupttypus or Nebentypus for small weights k and small prime stufe p.

We now furnish the coefficients $a_n(\cdot)$ of $\exp(2\pi inz)$ from $n=0$ to $n=33$ for the modular forms $\eta^2\eta_{11}^2, E_{1,3}, E_{2,3}$ and ϑ_3 since it was necessary to know the coefficients of q^{11}, q^{22}, q^{33} in the expansions of $\eta^2\eta_{11}^2E_{1,3}, \eta^2\eta_{11}^2E_{2,3}, \eta^2\eta_{11}^2\vartheta_3$ for our subsequent working. The coefficients $a_n(\cdot)$ are listed against the respective modular form in increasing order of n from 0 to 33:

$a_n(\eta^2\eta_{11}^2)$: 0, 1, −2, −1, 2, 1, 2, −2, 0, −2, −2, 1, −2, 4, 4, −1, −4, −2, 4, 0, 2, 2, −2, −1, 0, −4, −8, 5, −4, 0, 2, 7, 8, −1.

$a_n(E_{1,3})$: 0, 1, 3, 10, 13, 26, 30, 48, 51, 91, 78, 121, 130, 168, 144, 260, 205, 288, 273, 360, 338, 480, 363, 530, 510, 651, 504, 820, 624, 840, 780, 962, 819, 1210.

$a_n(E_{2,3})$: −3, 1, −3, 10, 13, 26, −30, −48, −51, 91, −78, 1, 130, −168, 144, 260, 205, −288, −273, −360, 338, −480, −3, 530, −510, 651, 504, 820, −624, −840, −780, 962, −819, 10.

$a_n(\vartheta_3)$: 0, 2, 0, −10, 8, −2, 0, 0, 0, 32, 0, −22, −40, 0, 0, 10, 32, 0, 0, 0, −8, 0, 0, 70, 0, −48, 0, −70, 0, 0, 0, −74, 0, 110.

Writing q for $\exp(2\pi iz)$, we also highlight those Fourier coefficients in the expansions of $E_{1,5}$, $E_{2,5}$, $f_1 := \eta^2\eta_{11}^2E_{1,3}$, $f_2 := \eta^2\eta_{11}^2E_{2,3}$ and $f_3 := \eta^2\eta_{11}^2\vartheta_3$ which are relevant to our proofs in the sequel:

$$E_{1,5}(z) = q + 15q^2 + 82q^3 + 241q^4 + \cdots + (11)^4q^{11} + \cdots,$$

$$E_{2,5}(z) = \frac{1275}{11} + q - 15q^2 + 82q^3 + 241q^4 + \cdots + q^{11} + \cdots,$$

$$f_1(z) = q^2 + q^3 + 3q^4 + \cdots - 11q^{11} + \cdots - 55q^{22} + \cdots + 154q^{33} + \cdots,$$

$$f_2(z) = -3q + 7q^2 - 2q^3 + 9q^4 + \cdots - 308q^{11} + \cdots - 1177q^{22} + \cdots - 407q^{33} + \cdots,$$

$$f_3(z) = 2q^2 - 4q^3 - 12q^4 + \cdots - 88q^{11} + \cdots + 286q^{22} + \cdots - 220q^{33} + \cdots. \tag{6}$$

In connection with the derivation of partition congruences for the moduli $\rho = 5, 7, 11$ etc., Ramanujan [7] applied to the relevant power-series

$$f(q) = \sum_{n=0}^{\infty} a_n q^n,$$

an operator U_ρ taking f to $U_\rho(f)$ defined by $(U_\rho(f))(q) := 1/\rho \sum_\zeta f(q^{1/\rho}\zeta)$ where the summation is over all the ρth roots of unity ζ; actually, $(U_\rho(f))(q)$ is nothing but $\sum_{n=0}^{\infty} a_{\rho n}q^n$. One may note that this operator U_ρ is essentially T_ρ^p considered (much later) by Hecke ([4], p. 839) on modular forms for $\Gamma_0(\rho)$. In the case of modular forms of Nebentypus $(-k, \rho, \varepsilon)$ in particular, the operator U_ρ maps the subspace generated by the two Eisenstein series into itself and the subspace of cusp forms into

itself. For the Eisenstein series $E_{1,5}$, $E_{2,5}$ of Nebentypus $(-5, 11, \varepsilon)$, we may thus write

$$U_{11}(E_{1,5}) = \alpha_1 E_{1,5} + \beta_1 E_{2,5}, \quad U_{11}(E_{2,5}) = \alpha_2 E_{1,5} + \beta_2 E_{2,5}$$

with constants α_i, β_j. On the other hand, by directly applying U_{11} to the Fourier expansions of $E_{1,5}$, $E_{2,5}$ in (6), we see that

$$U_{11}(E_{1,5}) = (11)^4 q + \cdots, \; U_{11}(E_{2,5}) = \tfrac{1275}{11} + q + \cdots$$

and a comparison of Fourier coefficients gives us immediately that $\alpha_1 = (11)^4$, $\beta_1 = 0$, $\alpha_2 = 0$, $\beta_2 = 1$ i.e.

$$U_{11}(E_{1,5}) = (11)^4 E_{1,5}, \quad U_{11}(E_{2,5}) = E_{2,5}. \tag{7}$$

From (6), it is clear that

$$U_{11}(f_1)(z) = -11q - 55q^2 + 154q^3 + \cdots$$

$$U_{11}(f_2)(z) = -308q - 1177q^2 - 407q^3 + \cdots$$

$$U_{11}(f_3)(z) = -88q + 286q^2 - 220q^3 + \cdots. \tag{8}$$

On the other hand, since f_1, f_2, f_3 generate the subspace of cusp forms of Nebentypus $(-5, 11, \varepsilon)$ which is preserved by U_{11}, we have, for suitable constants $\gamma_{i,j}$,

$$U_{11}(f_i) = \gamma_{i,1} f_1 + \gamma_{i,2} f_2 + \gamma_{i,3} f_3, \quad i = 1, 2, 3. \tag{9}$$

We solve for the constants $\gamma_{i,j}$ from the following equations obtained by equating the corresponding coefficients of q^n in $U_{11}(f_i)$ in the light of (9), (6) and (8):

$$-3\gamma_{1,2} = -11, \gamma_{1,1} + 7\gamma_{1,2} + 2\gamma_{1,3} = -55, \gamma_{1,1} - 2\gamma_{1,2} - 4\gamma_{1,3} = 154$$

$$-3\gamma_{2,2} = -308, \gamma_{2,1} + 7\gamma_{2,2} + 2\gamma_{2,3} = -1177, \gamma_{2,1} - 2\gamma_{2,2} - 4\gamma_{2,3} = -407$$

$$-3\gamma_{3,2} = -88, \gamma_{3,1} + 7\gamma_{3,2} + 2\gamma_{3,3} = 286, \gamma_{3,1} - 2\gamma_{3,2} - 4\gamma_{3,3} = -220.$$

We then obtain

$$\gamma_{1,1} = 0, \quad \gamma_{1,2} = 11/3, \quad \gamma_{1,3} = -121/3$$

$$\gamma_{2,1} = -1331, \quad \gamma_{2,2} = 308/3, \quad \gamma_{2,3} = -847/3$$

$$\gamma_{3,1} = 0, \quad \gamma_{3,2} = 88/3, \quad \gamma_{3,3} = 121/3$$

and therefore

$$U_{11}(f_1) = \tfrac{11}{3} f_2 - \tfrac{121}{3} f_3, \quad U_{11}(f_2) = -(11)^3 f_1 + \tfrac{308}{3} f_2 - \tfrac{847}{3} f_3,$$

$$U_{11}(f_3) = \tfrac{88}{3} f_2 + \tfrac{121}{3} f_3.$$

3. Two 'allied' modular identities

For Dedekind's η-function, we know that for every $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$,

$\eta((az+b)(cz+d)^{-1}) = \varepsilon(M)(cz+d)^{\frac{1}{2}}\eta(z)$ with a well-defined branch of $(cz+d)^{\frac{1}{2}}$ and a multiplier $\varepsilon(M)$ which is a 24th root of unity. If M is in $\Gamma_0(11)$, then $M_1 = \begin{pmatrix} 11 & 0 \\ 0 & 1 \end{pmatrix} M \begin{pmatrix} 1/11 & 0 \\ 0 & 1 \end{pmatrix}$ is in $SL_2(\mathbb{Z})$ and so $\eta_{11}((az+b)(cz+d)^{-1}) = \varepsilon_{11}(M) \times (cz+d)^{\frac{1}{2}}\eta_{11}(z)$ for every $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_0(11)$, with $\varepsilon_{11}(M) := \varepsilon(M_1)$. Using the fact that η^{24} is of Haupttypus $(-12, 1, 1)$ and $\eta^2\eta_{11}^2$ of Nebentypus $(-2, 11, \varepsilon_{11})$, it is not hard to see that $(\varepsilon^{11}(M_1)/\varepsilon(M))^2 = 1 = (\varepsilon^{11}(M)/\varepsilon(M_1))^2$ for every M in $\Gamma_0(11)$; further, we can verify that η_{11}^{11}/η and η^{11}/η_{11} are both of Nebentypus $(-5, 11, \varepsilon_{11})$.

Lemma. With $q = \exp(2\pi iz)$, *we have*

$$E_{1,3}(z) = \sum_{n=1}^{\infty} \left(\frac{n}{11}\right) \frac{q^n(1+q^n)}{(1-q^n)^3}, \quad E_{2,3}(z) = -3 + \sum_{n=1}^{\infty} \left(\frac{n}{11}\right) n^2 \frac{q^n}{1-q^n}$$

$$E_{1,5}(z) = \sum_{n=1}^{\infty} \left(\frac{n}{11}\right) \frac{q^n(1+11q^n+11q^{2n}+q^{3n})}{(1-q^n)^5},$$

$$E_{2,5}(z) = \frac{1275}{11} + \sum_{n=1}^{\infty} \left(\frac{n}{11}\right) n^4 \frac{q^n}{1-q^n}.$$

Proof. We give only the proof for the assertion involving $E_{1,5}$, since the proofs of the remaining three assertions are the same as that in ([6], Lemma on p. 226). Now $\sum_{j=0}^{3}(m+j)(m+j-1)(m+j-2)(m+j-3) = 4m^4 + 20m^2$ and for $|u| < 1$,

$$\frac{u^{4-j}}{(1-u)^5} = \sum_{m=j+1}^{\infty} \frac{m(m-1)(m-2)(m-3)}{4!} u^{m-j} \quad \text{for} \quad j = 0, 1, 2, 3.$$

Hence

$$\frac{6(u^4+u^3+u^2+u)}{(1-u)^5} = \sum_{m=1}^{\infty} m^4u^m + 5\sum_{m=1}^{\infty} m^2u^m$$

$$= \sum_{m=1}^{\infty} m^4u^m + 5\frac{u+u^2}{(1-u)^3}$$

as in ([6], Lemma) again i.e.

$$\frac{u^4+11u^3+11u^2+u}{(1-u)^5} = \sum_{m=1}^{\infty} m^4u^m, \quad \text{for} \quad |u| < 1.$$

Setting $u = q^r$ $(r = 1, 2, \ldots)$, multiplying both sides of the last identity by the Legendre symbol $\left(\frac{r}{11}\right)$ and summing over r from 1 to ∞, we obtain

$$\sum_{r,m\geq 1} \left(\frac{r}{11}\right) q^{mr} m^4 = \sum_{r=1}^{\infty} \left(\frac{r}{11}\right) \frac{q^r(1+11q^r+11q^{2r}+q^{3r})}{(1-q^r)^5}.$$

Our assertion for $E_{1,5}(z)$ is now immediate.

The following theorem gives the identities involving the two "allied" functions η_{11}^{11}/η

and η^{11}/η_{11}, which correspond for the modulus 11, to Ramanujan's identities (1)–(2) or (3)–(4) for 5 or 7 respectively.

Theorem. *We have the two "allied" identities:*

(i)
$$x^5\frac{\prod_{n=1}^{\infty}(1-x^{11n})^{11}}{\prod_{n=1}^{\infty}(1-x^n)}=\frac{3}{3825}\sum_{n=1}^{\infty}\left(\frac{n}{11}\right)\frac{x^n(1+11x^n+11x^{2n}+x^{3n})}{(1-x^n)^5}$$
$$-\left\{\frac{116}{3825}\sum_{n=1}^{\infty}\left(\frac{n}{11}\right)\frac{x^n(1+x^n)}{(1-x^n)^3}\right.$$
$$-\frac{1}{3825}\left(-3+\sum_{n=1}^{\infty}\left(\frac{n}{11}\right)n^2\frac{x^n}{1-x^n}\right)$$
$$\left.-\frac{32}{3825}\sum_{\mu\in\mathbb{Z}+\mathbb{Z}(1+\sqrt{-11})/2}\mu^2x^{\mu\bar{\mu}}\right\}$$
$$\times x\prod_{n=1}^{\infty}(1-x^n)^2(1-x^{11n})^2$$

(ii)
$$\frac{\prod_{n=1}^{\infty}(1-x^n)^{11}}{\prod_{n=1}^{\infty}(1-x^{11n})}=\frac{11}{1275}\left(\frac{1275}{11}+\sum_{n=1}^{\infty}\left(\frac{n}{11}\right)n^4\frac{x^n}{1-x^n}\right)$$
$$-\left\{\frac{(11)^4}{3825}\sum_{n=1}^{\infty}\left(\frac{n}{11}\right)\frac{x^n(1+x^n)}{(1-x^n)^3}\right.$$
$$-\frac{1276}{3825}\left(-3+\sum_{n=1}^{\infty}\left(\frac{n}{11}\right)n^2\frac{x^n}{1-x^n}\right)$$
$$\left.-\frac{3872}{3825}\sum_{\mu\in\mathbb{Z}+\mathbb{Z}(1+\sqrt{-11})/2}\mu^2x^{\mu\bar{\mu}}\right\}.$$
$$\times x\prod_{n=1}^{\infty}(1-x^n)^2(1-x^{11n})^2.$$

Proof. Since η_{11}^{11}/η and η^{11}/η_{11} are of Nebentypus $(-5,11,\varepsilon_{11})$ there exist constants $\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5$ and $\mu_1,\mu_2,\mu_3,\mu_4,\mu_5$ such that

$$\eta_{11}^{11}/\eta=\lambda_1E_{1,5}+\lambda_2E_{2,5}+\lambda_3\eta^2\eta_{11}^2E_{1,3}+\lambda_4\eta^2\eta_{11}^2E_{2,3}+\lambda_5\eta^2\eta_{11}^2\vartheta_3,$$
$$\eta^{11}/\eta_{11}=\mu_1E_{1,5}+\mu_2E_{2,5}+\mu_3\eta^2\eta_{11}^2E_{1,3}+\mu_4\eta^2\eta_{11}^2E_{2,3}+\mu_5\eta^2\eta_{11}^2\vartheta_3.$$

From (6) and the Fourier expansions

$$\eta_{11}^{11}(z)/\eta(z)=q^5+\cdots+11q^{11}+\cdots,$$
$$\eta^{11}(z)/\eta_{11}(z)=1-11q+44q^2-55q^3-110q^4+\cdots-2068q^{11}+\cdots,$$

we obtain the system of equations for λ_i, μ_j:

$$\lambda_2 = 0, \quad \lambda_1 + \lambda_2 - 3\lambda_4 = 0, \quad 15\lambda_1 - 15\lambda_2 + \lambda_3 + 7\lambda_4 + 2\lambda_5 = 0,$$

$$82\lambda_1 + 82\lambda_2 + \lambda_3 - 2\lambda_4 - 4\lambda_5 = 0, \quad 241\lambda_1 + 241\lambda_2 + 3\lambda_3 + 9\lambda_4 - 12\lambda_5 = 0,$$

$$\tfrac{1275}{11}\mu_2 = 1, \quad \mu_1 + \mu_2 - 3\mu_4 = -11, \quad 15\mu_1 - 15\mu_2 + \mu_3 + 7\mu_4 + 2\mu_5 = 44,$$

$$82\mu_1 + 82\mu_2 + \mu_3 - 2\mu_4 - 4\mu_5 = -55,$$

$$241\mu_1 + 241\mu_2 + 3\mu_3 + 9\mu_4 - 12\mu_5 = -110.$$

Solving these equations, we get

$$\lambda_1 = \tfrac{3}{3825}, \quad \lambda_2 = 0, \quad \lambda_3 = -\tfrac{116}{3825}, \quad \lambda_4 = \tfrac{1}{3825}, \quad \lambda_5 = \tfrac{32}{3825}$$

$$\mu_1 = 0, \quad \mu_2 = \tfrac{11}{1275}, \quad \mu_3 = -\frac{(11)^4}{3825}, \quad \mu_4 = \frac{(11)^2 \times 116}{3825}, \quad \mu_5 = \frac{(11)^3 \times 32}{3825}.$$

If we write x in lieu of q, the two "allied" identities are now an immediate consequence, in view of the Lemma above.

Together with (7) and (10), the theorem yields the

COROLLARY.

(i) $$U_{11}(\eta_{11}^{11}/\eta) = (11)^4 \eta_{11}^{11}/\eta + \frac{(11)^3}{3} f_1 - \tfrac{11}{3} f_2 - 121 f_3$$

(ii) $$U_{11}(\eta^{11}/\eta_{11}) = \eta^{11}/\eta_{11} - \frac{(11)^4}{3} f_1 + \frac{(11)^2 \times 17}{3} f_2 - \frac{(11)^3}{3} f_3.$$

Proof. Applying U_{11} to both sides of the identities

$$\eta_{11}^{11}/\eta = \tfrac{1}{3825}(3E_{1,5} - 116 f_1 + f_2 + 32 f_3)$$

$$\eta^{11}/\eta_{11} = \tfrac{1}{3825}(33E_{2,5} - (11)^4 f_1 + ((11)^2 \times 116) f_2 + ((11)^3 \times 32) f_3)$$

and using (7) and (10), we obtain, on substituting thereafter for $E_{1,5}$ in terms of η_{11}^{11}/η and for $E_{2,5}$ in terms of η^{11}/η_{11}, assertions (i) and (ii) of the Corollary, after simplification.

Remark 1. The Fourier coefficients in the expansions of $U_{11}(f_j)$, $j = 1, 2, 3$ are all integral clearly. However, it is not obvious why the coefficients of $\tfrac{11}{3} f_2 - \tfrac{121}{3} f_3$ or $\tfrac{308}{3} f_2 - \tfrac{847}{3} f_3$ or $\tfrac{88}{3} f_2 + \tfrac{121}{3} f_3$ are integral or equivalently, why the Fourier coefficients of $f_2 + f_3$ are all in $3\mathbb{Z}$. Actually, the Fourier coefficients of $E_{2,3} + \vartheta_3$ are already in $3\mathbb{Z}$, for purely arithmetical reasons. To see this fact independently, let us note first that the constant Fourier coefficient in $E_{2,3} + \vartheta_3$ is -3 while the Fourier coefficient of q^n for $n \geqslant 1$ is

$$\sum_{1 \leqslant d \mid n} d^2 \left(\frac{d}{11}\right) + \sum_{\substack{\mu\bar{\mu} = n \\ \mu \in o}} \mu^2$$

where $\mathfrak{a} := \mathbb{Z} + \mathbb{Z}\cdot\frac{1}{2}(1+\sqrt{-11})$. Let $n = n_1 \cdot 3^r$ with r the highest exponent such that 3^r divides n. Then evidently

$$\sum_{d|n} d^2\left(\frac{d}{11}\right) \equiv \sum_{d|n_1} d^2\left(\frac{d}{11}\right) (\mathrm{mod}\ 3).$$

When μ_j runs over μ in $\mathfrak{a}$ with $\mu\bar{\mu} = n_1$ and ν_k over μ in $\mathfrak{a}$ with $\mu\bar{\mu} = 3^r$, then $\mu_j\nu_k$ covers the set of μ in $\mathfrak{a}$ with $\mu\bar{\mu} = n$ twice, in view of $\mu_j\nu_k = (-\mu_j)(-\nu_k)$. Hence

$$\sum_{\substack{\mu\in\mathfrak{a}\\ \mu\bar{\mu}=n}} \mu^2 = \frac{1}{2} \sum_{\substack{\lambda\in\mathfrak{a}\\ \lambda\bar{\lambda}=n_1}} \lambda^2 \sum_{\substack{\mu\in\mathfrak{a}\\ \mu\bar{\mu}=3^r}} \mu^2.$$

Now

$$\sum_{\substack{\mu\bar{\mu}=n_1\\ \mu\in\mathfrak{a}}} \mu^2 \equiv \sum_{\substack{\mu\bar{\mu}=n_1\\ \mu\in\mathfrak{a}}} 1\ (\mathrm{mod}\ 3),$$

since $\mu = \frac{1}{2}(x+\sqrt{-11}y)$, $\mu\bar{\mu} = n_1, 3\nmid n_1$ together imply that $3\mid xy$ but $3\nmid(x,y)$ and

$$\sum_{\substack{x,y\in\mathbb{Z}\\ x^2+11y^2=4n_1}} \tfrac{1}{4}(x+\sqrt{-11}y)^2 = \sum_{\substack{x,y\in\mathbb{Z}\\ x^2+11y^2=4n_1}} \tfrac{1}{4}(x^2-11y^2)$$
$$\equiv \sum_{\substack{x,y\in\mathbb{Z}\\ x^2+11y^2=4n_1}} (x^2+y^2) \equiv \sum_{\substack{\mu\bar{\mu}=n_1\\ \mu\in\mathfrak{a}}} 1\ (\mathrm{mod}\ 3).$$

But

$$\sum_{\substack{\mu\bar{\mu}=n_1\\ \mu\in\mathfrak{a}}} 1 = 2 \sum_{1\leqslant d|n_1} \left(\frac{d}{11}\right)$$

since $\mathbb{Q}(\sqrt{-11})$ has class number 1 and has just 2 roots of unity. Also since

$$3\nmid n_1, 2 \sum_{1\leqslant d|n_1} \left(\frac{d}{11}\right) \equiv 2 \sum_{1\leqslant d|n_1} d^2\left(\frac{d}{11}\right) (\mathrm{mod}\ 3)$$

and as a consequence, we have

$$\sum_{\substack{\mu\bar{\mu}=n_1\\ \mu\in\mathfrak{a}}} \mu^2 \equiv 2 \sum_{1\leqslant d|n} d^2\left(\frac{d}{11}\right) (\mathrm{mod}\ 3).$$

On the other hand

$$\sum_{\substack{\mu\bar{\mu}=3^r\\ \mu\in\mathfrak{a}}} \mu^2 = \sum_{\substack{x,y\in\mathbb{Z}\\ x^2+11y^2=4\cdot 3^r}} \tfrac{1}{4}(x^2-11y^2) \equiv \sum_{\substack{x,y\in\mathbb{Z}\\ x^2+11y^2=4\cdot 3^r}} (x^2+y^2)$$
$$\equiv 2 \sum_{\substack{\mu\bar{\mu}=3^r\\ \mu\in\mathfrak{a}}} 1 \equiv 2 \sum_{\substack{\mu\bar{\mu}=3^r\\ 3\nmid\mu,\mu\in\mathfrak{a}}} 1\ (\mathrm{mod}\ 3).$$

But the number of μ in $\mathfrak{a}$ with $3\nmid\mu$ and $\mu\bar{\mu} = 3^r$ is just 4. Hence

$$\sum_{\substack{\mu\bar{\mu}=3^r\\ \mu\in\mathfrak{a}}} \mu^2 \equiv 2\ (\mathrm{mod}\ 3),$$

and as a result,

$$\sum_{\substack{\mu|i=n\\ \mu\in\alpha}} \mu^2 \equiv \sum_{\substack{\mu\in\alpha\\ \mu|i=n_1}} \mu^2 \equiv 2 \sum_{1\leqslant d|n} d^2\left(\frac{d}{11}\right) (\mathrm{mod}\ 3),$$

proving our assertion above.

Likewise, from the simple congruence relation

$$\sum_{1\leqslant d|n} d^2\left\{\left(\frac{d}{11}\right)-\left(\frac{n/d}{11}\right)\right\} \equiv \sum_{1\leqslant d|n_1} d^2\left\{\left(\frac{d}{11}\right)-\left(\frac{n_1/d}{11}\right)\right\}$$

$$\equiv \sum_{1\leqslant d|n_1}\left(\frac{d}{11}\right)-\sum_{1\leqslant d|n_1}\left(\frac{n_1/d}{11}\right) \equiv 0\,(\mathrm{mod}\ 3),$$

we see that $E_{1,3}-E_{2,3}$ and hence f_1-f_2 has all its Fourier coefficients in $3\mathbb{Z}$. It is no more a mystery as to why all the Fourier coefficients of the sum of the last three terms on the right hand side of assertion (ii) in the Corollary above are integral, since the Fourier coefficients of $f_1-2f_2-f_3$ are all in $3\mathbb{Z}$! In connection with congruences for Fourier coefficients of modular forms, we should refer to the recent interesting results due to J Sturm [9].

Remark 2. From the definition of U_{11}, it is easily seen that

$$U_{11}\left(\frac{q^5\prod_{n=1}^{\infty}(1-q^{11n})^{11}}{\prod_{n=1}^{\infty}(1-q^n)}\right) = U_{11}\left(\prod_{n=1}^{\infty}(1-q^{11n})^{11}\right)\cdot U_{11}\left(\frac{q^5}{\prod_{n=1}^{\infty}(1-q^n)}\right)$$

$$= \prod_{n=1}^{\infty}(1-q^n)^{11}\cdot U_{11}\left(q^5\sum_{n=0}^{\infty}p(n)q^n\right)$$

$$= \prod_{n=1}^{\infty}(1-q^n)^{11}\sum_{m=0}^{\infty}p(11m+6)q^{m+1}.$$

Hence, by assertion (i) of the Corollary above, we obtain

$$\sum_{m=0}^{\infty}p(11m+6)q^{m+1} = q^5\frac{\prod_{m=1}^{\infty}(1-q^{11m})^{11}}{\prod_{m=1}^{\infty}(1-q^m)^{12}}$$

$$\times\left\{(11)^4+\frac{(11)^3E_{1,3}-11E_{2,3}-363\vartheta_3}{3q^4\prod_{n=1}^{\infty}(1-q^{11n})^9\Big/\prod_{n=1}^{\infty}(1-q^n)^3}\right\}.$$

This may be seen to be equivalent to identity (3.25) derived in ([3], p. 158) after "lengthy but elementary" calculations (that have, however, been suppressed), as soon as we check that α,β can be identified respectively with $(2E_{1,3}-\vartheta_3)/6(\eta_{11}^9/\eta^3)$,

$E_{1,3}/(\eta_{11}^9/\eta^3)$. The infinite products occurring on the right hand side of the identity just stated above have expansions as power-series in q with constant term 1 and other coefficients in $\mathbb{Z}$. Hence the right hand side of this identity is a power-series in q with coefficients in $11\mathbb{Z}$. As a result, the well-known partition congruences $p(11m+6) \equiv 0 \pmod{11}$ due to Ramanujan become evident. Partition congruences for a higher modulus, say $(11)^2$ may also be obtained therefrom; for example, if a_m is the coefficient of q^{m-1} in

$$E_{2,3} \prod_{n=1}^{\infty} \frac{(1-q^{11n})^2}{(1-q^n)^9},$$

then $p(11m+6) + 44a_m \equiv 0 \pmod{(11)^2}$.

Remark 3. Following Newman [5], let $p_r(n)$ denote the coefficient of q^n in $\prod_{m=1}^{\infty}(1-q^m)^r$. Now

$$U_{11}(\eta^{11}/\eta_{11}) = U_{11}\left(\sum_{n=0}^{\infty} p_{11}(n)q^n\right) \Big/ \prod_{n=1}^{\infty}(1-q^n)$$

$$= \left(\sum_{n=0}^{\infty} p_{11}(11n)q^n\right) \Big/ \prod_{n=1}^{\infty}(1-q^n).$$

On the other hand, we know that

$$U_{11}(\eta^{11}/\eta_{11}) = \tfrac{11}{12^{75}} U_{11}(E_{2,5}) - \frac{(11)^2}{3825}((11)^2 U_{11}(f_1) - 116U_{11}(f_2) - 352U_{11}(f_3)).$$

Therefore

$$\sum_{n=0}^{\infty} p_{11}(11n)q^n = \prod_{n=1}^{\infty}(1-q^n) \times \left\{\tfrac{11}{12^{75}} E_{2,5} - \frac{11^2}{3825}((11)^2 U_{11}(f_1) - 116U_{11}(f_2) - 352U_{11}(f_3))\right\}$$

giving us the congruence

$$p_{11}(11n) \equiv p_1(n) - 11 \sum_{r=1}^{n} p_1(n-r) \sum_{1 \leqslant d \mid r} d^4 \left(\frac{d}{11}\right) \pmod{(11)^2}$$

and in particular, the classical congruence $p_{11}(11n) \equiv p_1(n) \pmod{11}$.

4. Ramanujan's proof for partition congruences modulo 11

In this section, we present the proof for the congruences $p(11n+6) \equiv 0 \pmod{11}$ given tersely by Ramanujan in [7], along with proofs for the case of the moduli 5, 7, 49, 121, 23 etc.

Writing

$$P = 1 - 24 \sum_{n=1}^{\infty} \left(\sum_{1 \leqslant d \mid n} d \right) \exp(2\pi i n z), \quad Q = 1 + 240 \sum_{n=1}^{\infty} \left(\sum_{1 \leqslant d \mid n} d^3 \right) \exp(2\pi i n z),$$

$$R = 1 - 504 \sum_{n=1}^{\infty} \left(\sum_{1 \leqslant d \mid n} d^5 \right) \exp(2\pi i n z),$$

we know that QR is just the normalized Eisenstein series of weight 10 for the modular group, namely

$$QR = 1 - 264 \sum_{n=1}^{\infty} \left(\sum_{1 \leqslant d \mid n} d^9 \right) \exp(2\pi i n z).$$

Also, the normalized Eisenstein series E_{12} of weight 12, given by

$$E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1} \left(\sum_{1 \leqslant d \mid n} d^{11} \right) \exp(2\pi i n z)$$

is a linear combination of Q^3 and R^2 which generate the space of modular forms of weight 12 for the modular group; indeed, with $q := \exp(2\pi i z)$,

$$691 + 65520 \sum_{n=1}^{\infty} q^n \left(\sum_{1 \leqslant d \mid n} d^{11} \right) = 441 Q^3 + 250 R^2. \tag{11}$$

Given any natural number m and two power series

$$R_1 = \sum_{n=0}^{\infty} a_n q^n, \quad R_2 = \sum_{n=0}^{\infty} b_n q^n,$$

with all a_n, b_n integral, we write $R_1 \equiv R_2 \pmod{m}$ whenever $a_n \equiv b_n \pmod{m}$ for all $n \geqslant 0$. Using the congruence $d^{11} \equiv d \pmod{11}$ for every integer d, we note that the left hand side of (11) is $\equiv -2P \pmod{11}$ while the right hand side is $\equiv Q^3 - 3R^2 \pmod{11}$. Thus we have

$$Q^3 - 3R^2 \equiv -2P \pmod{11}. \tag{12}$$

It is also clear that

$$QR \equiv 1 \pmod{11}. \tag{13}$$

As a consequence,

$$\begin{aligned}
(Q^3 - R^2)^5 &= (Q^3 - 3R^2)^5 + 10(Q^3 - 3R^2)^4 R^2 + 40(Q^3 - 3R^2)^3 R^4 \\
&\quad + 80(Q^3 - 3R^2)^2 R^6 + 80(Q^3 - 3R^2) R^8 + 32 R^{10} \\
&\equiv (Q^3 - 3R^2)^5 - (Q^3 - 3R^2)^4 R^2 + 7(Q^3 - 3R^2)^3 R^4 \\
&\quad + 3(Q^3 - 3R^2)^2 R^6 + 3(Q^3 - 3R^2) R^8 - R^{10} \pmod{11} \\
&\equiv (Q^3 - 3R^2)^5 + (Q^3 - 3R^2)^3 R^2 (-Q^3 + 10R^2) \\
&\quad + 3(Q^3 - 3R^2)^2 R^6 + 3(Q^3 - 3R^2) R^8 - R^{10} \pmod{11}
\end{aligned}$$

$$\equiv (Q^3-3R^2)^5 - Q(Q^3-3R^2)^3 - (Q^3-3R^2)^3 R^4$$
$$+ 3(Q^3-3R^2)^2 R^6 + 3(Q^3-3R^2)R^8 - R^{10} \pmod{11}, \text{ by (13)}$$
$$\equiv (Q^3-3R^2)^5 - Q(Q^3-3R^2)^3 - (Q^3-3R^2)^2 R^4 (Q^3-3R^2)$$
$$+ 3(Q^3-3R^2)R^8 - R^{10} \pmod{11}$$
$$\equiv (Q^3-3R^2)^5 - Q(Q^3-3R^2)^3 - R(Q^3-3R^2)^2$$
$$+ (Q^3-3R^2)(R^6(6Q^3-18R^2)+3R^8) - R^{10} \pmod{11}$$
$$\equiv (Q^3-3R^2)^5 - Q(Q^3-3R^2)^3 - R(Q^3-3R^2)^2$$
$$+ (Q^3-3R^2)(6Q^3+7R^2)R^6 - R^{10} \pmod{11}$$
$$\equiv (Q^3-3R^2)^5 - Q(Q^3-3R^2)^3 - R(Q^3-3R^2)^2$$
$$+ 6Q^6R^6 - 11Q^3R^8 - 22R^{10} \pmod{11}$$
$$\equiv (Q^3-3R^2)^5 - Q(Q^3-3R^2)^3 - R(Q^3-3R^2)^2$$
$$- 5QR \pmod{11} \tag{14}$$

since $6Q^6R^6 \equiv 6 \equiv -5 \equiv -5QR \pmod{11}$. By (12) and (14), we have

$$(Q^3-R^2)^5 \equiv -32P^5 + 8QP^3 - 4RP^2 - 5QR \pmod{11}$$
$$\equiv P^5 - 3P^3Q - 4P^2R - 5QR \pmod{11}. \tag{15}$$

We have, on the other hand, the well-known Ramanujan differential equations

$$q\frac{dP}{dq} = \tfrac{1}{12}(P^2-Q), \quad q\frac{dQ}{dq} = \tfrac{1}{3}(PQ-R), \quad q\frac{dR}{dq} = \tfrac{1}{2}(PR-Q^2) \tag{16}$$

which are of fundamental importance for the theory of p-adic modular forms due to Serre [8]. From (16), we have immediately the congruences

$$q\frac{dP}{dq} \equiv P^2 - Q, \quad q\frac{dQ}{dq} \equiv 4(PQ-R), \quad q\frac{dR}{dq} \equiv 6(PR-Q^2) \pmod{11}. \tag{17}$$

Now (15) and (17) imply without difficulty that

$$(Q^3-R^2)^5 \equiv q\frac{d}{dq}(3P^4 + 7P^2Q + 5PR) \pmod{11}. \tag{18}$$

But

$$(Q^3-R^2) = 1728q\prod_{n=1}^{\infty}(1-q^n)^{24} \equiv q\prod_{n=1}^{\infty}(1-q^n)^{24} \pmod{11}$$

so that

$$(Q^3-R^2)^5 \equiv q^5\prod_{n=1}^{\infty}(1-q^n)^{120} \pmod{11}. \tag{19}$$

Since

$$q^5\prod_{n=1}^{\infty}(1-q^n)^{120}=q^5\prod_{n=1}^{\infty}(1-q^n)^{121}\Big/\prod_{n=1}^{\infty}(1-q^n)$$

$$=\prod_{n=1}^{\infty}(1-q^n)^{121}\sum_{n=0}^{\infty}p(n)q^{n+5}$$

$$\equiv\prod_{n=1}^{\infty}(1-q^{121n})\sum_{n=0}^{\infty}p(n)q^{n+5}\pmod{11}$$

and since, further, the coefficient of q^{11m} in $q(\mathrm{d}/\mathrm{d}q)(\sum_{n=0}^{\infty}c_nq^n)$ with c_n in $\mathbb{Z}$ is $11mc_{11m}\equiv 0\pmod{11}$, we obtain from (18) and (19), the required congruence $p(11m-5)\equiv 0\pmod{11}$ for $m\geqslant 1$.

Without using the differential equations (16), Ramanujan derives directly from (15) and four other congruences, the general congruence relation

$$p(n-5)-p(n-126)-p(n-247)+p(n-610)+p(n-852)-\cdots$$

$$+n^4\sum_{d|n}d-3n^3\sum_{d|n}d^3-3n^2\sum_{d|n}d^5+5n\sum_{d|n}d^7\equiv 0\pmod{11}$$

which, of course, implies the simpler congruence $p(11n-5)\equiv 0\pmod{11}$ for $n\geqslant 1$.

References

[1] Bailey W N, A note on two of Ramanujan's formulae, *Q. J. Math.* **3** (1952) 29–31

[2] Bailey W N, A further note on two of Ramanujan's formulae, *Q. J. Math.* **3** (1952) 158–160

[3] Fine N J, On a system of modular functions connected with the Ramanujan identities, *Tohoku Math. J.* **8** (1956) 149–164

[4] Hecke E, Gesammelte Abhandlungen, van den Hoeck u. Ruprecht, Göttingen (1959)

[5] Newman M, A table of the coefficients of the powers of $\eta(\tau)$, *Indagationes Math.* **18** (1956) 204–216

[6] Raghavan S, On certain identities due to Ramanujan, *Q. J. Math.* **37** (1986) 221–229

[7] Ramanujan S, Congruence properties of $p(n)$ (unpublished manuscript) Trinity College Library (1920)

[8] Serre J P, Formes modulaires et fonctions zêta p-adiques, in *Modular functions of one variable III*—Springer Verlag—Lecture Notes in Mathematics (1973) pp. 191–268

[9] Sturm J, On the congruence of modular forms, in: *Number theory*—Springer Verlag—Lecture Notes in Mathematics (1985) p. 1240

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 277–290.

Hypergeometric series and continued fractions

K G RAMANATHAN
A1 Sree Krishna Dham, 70 L B S Marg, Bombay 400 080, India

Abstract. Ramanujan's results on continued fractions are simple consequences of three-term relations between hypergeometric series. Their q-analogues lead to many of the continued fractions given in the 'Lost' notebook in particular the famous one considered by Andrews and others.

Keywords. Hypergeometric series; continued fractions; q-series; Lost Notebook; three-term relations; modular functions.

1. Introduction

The hypergeometric series

$$f(\alpha, \beta; \gamma, x) = \sum_{m=0}^{\infty} \frac{(\alpha)_m (\beta)_m}{(1)_m \cdot (\gamma)_m} x^m, \tag{1}$$

where, for any α and rational integer m,

$$(\alpha)_m = \frac{\Gamma(\alpha + m)}{\Gamma(\alpha)},$$

was first discussed extensively by Gauss [6] who showed that any three contiguous series (see definition below) satisfy a linear relation. By suitable choice of these contiguous series, Gauss obtained continued fraction representations for ratios of hypergeometric series. Euler earlier had considered the integral

$$F(\alpha, \beta; \gamma, x) = \int_0^1 t^{\beta-1}(1-t)^{\gamma-\beta-1}(1-tx)^{-\alpha}\,dt \tag{2}$$

and by partial integration obtained a linear relation between three such integrals and then a continued fraction for the ratio of such integrals. This continued fraction is different from that of Gauss. Since it is easy to see that

$$F(\alpha, \beta; \gamma, x) = \frac{\Gamma(\beta)\Gamma(\gamma - \beta)}{\Gamma(\gamma)} f(\alpha, \beta; \gamma, x), \tag{3}$$

Euler's continued fraction is actually one related to contiguous hypergeometric series.

In the middle of the last century Heine, taking his cue from Jacobi and Eisenstein, considered in detail the so-called basic hypergeometric series

$$\varphi(\alpha, \beta; \gamma, q, x) = \sum_{m=0}^{\infty} \frac{(\alpha, q)_m \cdot (\beta, q)_m}{(q, q)_m \cdot (\gamma, q)_m} x^m, \tag{4}$$

where q is a parameter with $|q| < 1$ and for any α and rational integer m,

$$(\alpha, q)_m = (\alpha, q)_\infty / (\alpha q^m, q)_\infty \tag{5}$$

and

$$(\alpha, q)_\infty = (1-\alpha)(1-\alpha q)\cdots = \prod_{m=0}^{\infty} (1-\alpha q^m). \tag{6}$$

Heine [8] found all the three-term relations for φ, analogous to those found by Gauss for f and had obtained related continued fractions.

Ramanujan's researches in mathematics during the years 1903–1913 were recorded in his famous Notebooks. From these it became known that Ramanujan had not only rediscovered many of the classical results of Gauss, Euler, Heine and others on hypergeometric series and continued fractions but also found many new ones on these topics using systematically the three-term relations. There are many such related to Heine's q-series in the 'Lost' Notebook [13] discovered in 1976 by G E Andrews among the Ramanujan papers in the Trinity College, Cambridge.

Our object in this note is to show that many of the results of Ramanujan on continued fractions can be obtained as limiting cases of results of Gauss, Euler and Heine. In particular the famous continued fraction of Rogers–Ramanujan–Schur is a limiting case of Heine's q-analogue of Gauss' continued fraction. Some of the q-continued fractions are related to modular functions. The exploitation of this relationship between modular functions and continued fractions is one of the most beautiful aspects of Ramanujan's work on continued fractions. We do not go into details about this in the present paper, however.

2. Three-term relations

Ramanujan had seen Gauss' continued fraction stated in Carr's book (Synopsis of pure mathematics, London and Cambridge 1886). He studied, perhaps, elements of hypergeometric series from Chrystal's Algebra and Greenhills' Elliptic functions. In any case he must have derived the three-term relations in Gauss' memoir and others which he needed for his work.

From (1) we see that

$$f(\alpha, \beta; \gamma, x) = 1 + \frac{\alpha\cdot\beta}{1\cdot\gamma}\cdot x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot 2\cdot\gamma(\gamma+1)} x^2 + \cdots.$$

We say that $f(\alpha, \beta; \gamma, x)$ and $f(\alpha', \beta'; \gamma', x)$ are contiguous if

$$\alpha \equiv \alpha', \quad \beta \equiv \beta', \quad \gamma \equiv \gamma' \pmod 1.$$

Using three-term relations between contiguous hypergeometric series Gauss obtained a continued fraction for the ratio,

$$\frac{f(\alpha, \beta+1; \gamma+1, x)}{f(\alpha, \beta; \gamma, x)}.$$

Ramanujan gives it in the form

$$\frac{\alpha\beta x}{\gamma}\frac{f(\gamma-\alpha,\beta+1;\gamma+1,-x)}{f(\gamma-\alpha,\beta;\gamma,-x)}=\frac{\alpha\beta x}{\gamma+}\frac{(\alpha-\gamma)(\beta-\gamma)x}{\gamma+1+}\frac{(\alpha+1)(\beta+1)x}{\gamma+2+}\cdots. \tag{7}$$

The right side of (7) is symmetrical in α and β. This result is Entry 18 in Vol. 1, p. 215.

Entry 19 on the same page consists of three statements, all limiting cases. They are

$$\begin{aligned}\frac{\beta x}{\gamma}f(\beta+1,1;\gamma+1,-x)&=\frac{\beta x}{\gamma+}\frac{(\beta+1)\gamma x}{\gamma+1+}\frac{(\gamma-\beta)x}{\gamma+2+}\cdots\\&=\frac{\beta x}{\gamma+}\frac{(\beta+1)x}{1+}\frac{1\cdot(1+x)}{\gamma+}\frac{(\beta+2)x}{1+}\cdots\\&=\frac{\beta x}{\gamma+x(\beta+1)-}\frac{1\cdot(\beta+1)x(x+1)}{\gamma+1+x(\beta+3)-}\frac{2\cdot(\beta+2)x(x+1)}{\gamma+2+x(\beta+5)-}\cdots.\end{aligned} \tag{8}$$

Clearly the first of these relations is a special case of (7) obtained by putting $\beta=0,\gamma-\alpha$ for α and $\beta+1$ for α.

In order to obtain the second result, consider the two three-term relations

$$f(\alpha,\beta;\gamma,x)=\begin{cases}f(\alpha,\beta+1;\gamma,x)-\dfrac{\alpha x}{\gamma}f(\alpha+1,\beta+1;\gamma+1,x)\\[2ex]\dfrac{\gamma-\beta}{\gamma}f(\alpha+1,\beta;\gamma+1,x)+\dfrac{\beta(1-x)}{\gamma}f(\alpha+1,\beta+1;\gamma+1,x)\end{cases} \tag{9}$$

of which the first one is due to Gauss. In order to obtain the second one apply the formula

$$f(\alpha,\beta;\gamma,x)=(1-x)^{\gamma-\alpha-\beta}f(\gamma-\alpha,\gamma-\beta;\gamma,x) \tag{10}$$

to both sides of Gauss' relation

$$f(\alpha,\beta;\gamma,x)-f(\alpha,\beta;\gamma+1,x)=\frac{\alpha\beta x}{\gamma(\gamma+1)}f(\alpha+1,\beta+1;\gamma+2,x).$$

One then has

$$\begin{aligned}f(\alpha,\beta;\gamma,x)&=(1-x)f(\alpha+1,\beta+1;\gamma+1,x)\\&\quad+\frac{(\gamma-\alpha)(\gamma-\beta)x}{\gamma(\gamma+1)}f(\alpha+1,\beta+1;\gamma+2,x).\end{aligned} \tag{11}$$

Eliminate $f(\alpha+1,\beta+1;\gamma+2,x)$ between (11) and Gauss' relation

$$f(\alpha,\beta;\gamma,x)=f(\alpha+1,\beta;\gamma+1,x)-\frac{\beta(\gamma-\alpha)x}{\gamma(\gamma+1)}f(\alpha+1,\beta+1;\gamma+2,x).$$

We then obtain the second result in (9).

From the two relations in (9) one obtains

$$\frac{f(\alpha,\beta+1;\gamma,x)}{f(\alpha,\beta;\gamma,x)}=\frac{1}{1-\gamma-\beta-1+}\frac{\alpha x}{}\frac{(\beta+1)(1-x)}{1-}\frac{(\alpha+1)x}{\gamma-\beta-1+}\frac{(\beta+2)(1-x)}{1-}\cdots. \tag{12}$$

Putting $\beta=0$, changing α into $\beta+1$, γ into $\gamma+1$ and x into $-x$, we obtain the second formula in (8).

The last relation is obtained easily from the Gauss relation [6],

$$f(\alpha,\beta;\gamma,x)=\frac{\gamma-(\alpha+\beta+1)x}{\gamma}f(\alpha+1,\beta+1;\gamma+1,x)$$
$$+\frac{(\alpha+1)(\beta+1)(x-x^2)}{\gamma(\gamma+1)}f(\alpha+2,\beta+2;\gamma+2,x). \tag{13}$$

This result does not seem to have been noticed. It leads to the continued fraction

$$\frac{f(\alpha+1,\beta+1;\gamma+1,x)}{f(\alpha,\beta;\gamma,x)}=\frac{\gamma}{\gamma-(\alpha+\beta+1)x+}\frac{(\alpha+1)(\beta+1)(x-x^2)}{\gamma+1-(\alpha+\beta+3)x+}$$
$$\frac{(\alpha+2)(\beta+2)(x-x^2)}{\gamma+2-(\alpha+\beta+5)x+\cdots}. \tag{14}$$

If as before we put $\beta=0$, β for α and $-x$ for x, we obtain the third result in (8).

Ramanujan found another continued fraction from a three-term relation between

$$f(\alpha,\beta;\gamma,x),\quad f(\alpha+1,\beta;\gamma+1,x),\quad f(\alpha+2,\beta;\gamma+2,x).$$

It is clear from the form of the three series, that such a relation can be obtained from (13) by using the relation

$$(1-x)^{-\alpha}f\left(\alpha,\beta;\gamma,\frac{x}{x-1}\right)=f(\alpha,\gamma-\beta;\gamma,x) \tag{15}$$

on both sides of the relation (14). We obtain the relation

$$f(\alpha,\beta;\gamma,x)=\frac{\gamma+(\alpha-\beta+1)x}{\gamma}f(\alpha+1,\beta;\gamma+1,x)$$
$$-\frac{(\alpha+1)(\gamma-\beta+1)x}{\gamma(\gamma+1)}f(\alpha+2,\beta;\gamma+2,x). \tag{16}$$

This leads at once to the continued fraction

$$\frac{f(\alpha+1,\beta;\gamma+1,x)}{f(\alpha,\beta;\gamma,x)}=\frac{\gamma}{\gamma+(1+\alpha-\beta)x-}\ \frac{(\alpha+1)(1+\gamma-\beta)x}{\gamma+1+(2+\alpha-\beta)x-}$$

$$\frac{(\alpha+2)(2+\gamma-\beta)x}{\gamma+2+(3+\alpha-\beta)x-\cdots}. \tag{17}$$

This formula is *not* given in chapter XIV of Volume 1 which is devoted to continued fractions. It is given on page 198 of the same volume.

It is to be noted that the two formulae (10) and (15) are also given in Ramanujan's Notebook I (p. 193, Entry 11 and p. 191, Entry 4).

We shall state one another continued fraction whose q-analogue Ramanujan perhaps used. It depends on the three-term relations

$$f(\alpha,\beta;\gamma,x)=f(\alpha,\beta+1;\gamma,x)-\frac{\alpha x}{\gamma}f(\alpha+1,\beta+1;\gamma+1,x) \tag{18}$$

and the relation (16). We then have

$$\frac{f(\alpha,\beta;\gamma,x)}{f(\alpha,\beta+1;\gamma,x)}=1-\frac{\alpha x}{\gamma}\left(\frac{f(\alpha+1,\beta+1;\gamma+1,x)}{f(\alpha,\beta+1;\gamma,x)}\right).$$

We now substitute the continued fraction (17) for

$$\frac{\gamma f(\alpha,\beta+1;\gamma,x)}{f(\alpha+1,\beta+1;\gamma+1,x)}.$$

We then obtain

$$\frac{f(\alpha,\beta+1;\gamma,x)}{f(\alpha,\beta;\gamma,x)}=\frac{1}{1-}\ \frac{\alpha x}{\gamma+(\alpha-\beta)x-}\ \frac{(\alpha+1)(\gamma-\beta)x}{\gamma+1+(\alpha-\beta+1)x-}$$

$$\frac{(\alpha+2)(\gamma-\beta+1)x}{\gamma+2+(\alpha-\beta+2)x-\cdots}. \tag{19}$$

The interest in this is that after the first step everything else is like in the Euler continued fraction (17). In fact this can be easily generalized.

Hence by choosing suitable three-term relations one can get an infinity of continued fraction representations for the same ratio of two contiguous hypergeometric series.

3. Evaluation for special x

A second type of results on continued fractions concerns evaluation of these for special values of the variable x, say for

$$x=-1.$$

It is then clear that one would use the Kummer theorem

$$f(\alpha,\beta;1+\alpha-\beta,-1)=\frac{\Gamma(1+\alpha-\beta)\Gamma\left(1+\frac{\alpha}{2}\right)}{\Gamma(1+\alpha)\Gamma\left(1+\frac{\alpha}{2}-\beta\right)}. \tag{20}$$

This theorem of Kummer's is also in the Notebooks of Ramanujan (Vol. 1, p. 179, chapter XIV, Entry 24).

We take the continued fraction (19) with $x=-1$. We have

$$\frac{f(\alpha+1,\beta;\gamma+1,-1)}{f(\alpha,\beta;\gamma,-1)}=\frac{\gamma}{\gamma+\beta-\alpha-1+}\frac{(\alpha+1)(1+\gamma-\beta)}{\gamma+\beta-\alpha-1+}$$

$$\frac{(\alpha+2)(2+\gamma-\beta)}{\gamma+\beta-\alpha-1+\cdots}. \tag{21}$$

In order to be able to evaluate the left side of (21) using (20) it is necessary to impose some conditions on α,β,γ. Let us take

$$\beta=\alpha+\gamma. \tag{22}$$

Then

$$f(\beta,\alpha+1;\beta-\alpha,-1)=\frac{1}{2}\cdot\frac{\Gamma(\beta-\alpha)\cdot\Gamma\left(\frac{\beta}{2}\right)}{\Gamma(\beta)\Gamma\left(\frac{\beta}{2}-\alpha\right)}.$$

$$f(\beta+1,\alpha+1;\beta-\alpha+1,-1)=\frac{\beta-\alpha}{2\beta}\frac{\Gamma(\beta-\alpha)\Gamma\left(\frac{\beta+1}{2}\right)}{\Gamma(\beta)\Gamma\left(\frac{\beta+1}{2}-\alpha\right)}.$$

These two lead to

$$f(\beta,\alpha;\beta-\alpha,-1)=\frac{1}{2}\cdot\frac{\Gamma(\beta-\alpha)}{\Gamma(\beta)}\left(\frac{\Gamma\left(\frac{\beta}{2}\right)}{\Gamma\left(\frac{\beta}{2}-\alpha\right)}+\frac{\Gamma\left(\frac{\beta+1}{2}\right)}{\Gamma\left(\frac{\beta+1}{2}-\alpha\right)}\right).$$

This along with

$$f(\beta,\alpha;\beta-\alpha+1,-1)=\frac{\beta-\alpha}{2\beta}\frac{\Gamma(\beta-\alpha)\Gamma\left(\frac{\beta+1}{2}\right)}{\Gamma(\beta)\Gamma\left(\frac{\beta+1}{2}-\alpha\right)}$$

gives

$$f(\beta,\alpha+1;\beta-\alpha+1,-1)=\frac{1}{2\alpha}\frac{\Gamma(\beta-\alpha)}{\Gamma(\beta)}\left(\frac{\Gamma\left(\frac{\beta+1}{2}\right)}{\Gamma\left(\frac{\beta+1}{2}-\alpha\right)}-\frac{\Gamma\left(\frac{\beta}{2}\right)}{\Gamma\left(\frac{\beta}{2}-\alpha\right)}\right).$$

We have hence the following result:

$$\frac{1}{\alpha}\frac{\Gamma\left(\frac{\beta+1}{2}\right)\Gamma\left(\frac{\beta}{2}-\alpha\right)-\Gamma\left(\frac{\beta}{2}\right)\Gamma\left(\frac{\beta+1}{2}-\alpha\right)}{\Gamma\left(\frac{\beta+1}{2}\right)\Gamma\left(\frac{\beta}{2}-\alpha\right)+\Gamma\left(\frac{\beta}{2}\right)\Gamma\left(\frac{\beta+1}{2}-\alpha\right)}$$

$$=\frac{\beta-\alpha}{2(\beta-\alpha)-1+}\frac{1^2-\alpha^2}{2(\beta-\alpha)-1+}\frac{2^2-\alpha^2}{2(\beta-\alpha)-1+}\cdots. \tag{23}$$

In a similar way, if we put

$$1+\beta=\alpha+\gamma \tag{24}$$

the computations are a little bit simpler. Since

$$\gamma+\beta-\alpha-1=2(\beta-\alpha)$$

$$(\alpha+k)(k+\gamma-\beta)=\tfrac{1}{4}((2k+1)^2-(2\alpha-1)^2)$$

we have

$$\frac{f(\beta,\alpha+1;\beta-\alpha+2,-1)}{f(\beta,\alpha;\beta-\alpha+1,-1)}=\frac{(1+\beta-\alpha)(\beta-2\alpha)}{\alpha(1-\alpha)}\frac{\Gamma\left(\frac{\beta+1}{2}\right)\Gamma\left(\frac{\beta}{2}-\alpha\right)}{\Gamma\left(\frac{\beta+1}{2}-\alpha\right)\Gamma\left(\frac{\beta}{2}\right)}$$

$$+\frac{(1+\beta-\alpha)(\alpha-\beta)}{\alpha(1-\alpha)}.$$

If therefore we set

$$2\alpha-1=N,\quad 2(\beta-\alpha)=x>0,$$

we have Ramanujan's result (Vol. 1, p. 217, Entry 21), due originally to Euler and Stieltjes

$$\frac{4}{x+}\frac{1^2-N^2}{2x+}\frac{3^2-N^2}{2x+}\frac{5^2-N^2}{2x+}\cdots=\frac{\Gamma\left(\frac{x+N+1}{4}\right)\Gamma\left(\frac{x-N+1}{4}\right)}{\Gamma\left(\frac{x+N+3}{4}\right)\Gamma\left(\frac{x-N+3}{4}\right)}. \tag{25}$$

The results (23) and (25) are in a certain sense, complementary

4. Theorems of Perron and Ramanujan

We have seen several continued fraction representions for the same ratio of hypergeometric series. There is also a continued fraction representation which combines both the features of the Gauss method and the Euler method. The Gauss

method depends on two three-term relations

$$f(\alpha,\beta;\gamma,x)=\begin{cases} f(\alpha+1,\beta;\gamma+1,x)-\dfrac{\beta(\gamma-\alpha)x}{\gamma(\gamma+1)}f(\alpha+1,\beta+1;\gamma+2,x) \\ f(\alpha,\beta+1;\gamma+1,x)-\dfrac{\alpha(\gamma-\beta)x}{\gamma(\gamma+1)}f(\alpha+1,\beta+1;\gamma+2,x) \end{cases} \tag{26}$$

and the Euler method depends on one relation (16). If we use the first equation in (26), then

$$\frac{\gamma f(\alpha,\beta;\gamma,x)}{f(\alpha+1,\beta;\gamma+1,x)}=\gamma-\frac{\beta(\gamma-\alpha)}{\gamma+1}\left(\frac{f(\alpha+1,\beta;\gamma+1,x)}{f(\alpha+1,\beta+1;\gamma+2,x)}\right)^{-1}.$$

Using now the second equation in (26)

$$(\gamma+1)\frac{f(\alpha+1,\beta;\gamma+1,x)}{f(\alpha+1,\beta+1;\gamma+2,\alpha)}=\gamma+1-\frac{(\alpha+1)(\gamma+1-\beta)}{\gamma+2}\times\left(\frac{f(\alpha+1,\beta+1;\gamma+2,x)}{f(\alpha+2,\beta+1,\gamma+3,x)}\right)^{-1}.$$

We now use (16) for

$$(\gamma+2)\frac{f(\alpha+1,\beta+1;\gamma+2,x)}{f(\alpha+2,\beta+1;\gamma+3,x)}$$

with α,β,γ replaced by $\alpha+1$, $\beta+1$ and $\gamma+2$. We then get

$$\gamma+(1+\alpha-\beta)x-\frac{(\alpha+1)(1+\gamma-\beta)x}{\gamma+1+(2+\alpha-\beta)x-}\frac{(\alpha+2)(2+\gamma-\beta)x}{\gamma+2+(3+\alpha-\beta)x-}\cdots$$

$$=\gamma-\frac{\beta(\gamma-\alpha)x}{\gamma+1-}\frac{(\alpha+1)(\gamma+1-\beta)x}{\gamma+2+(1+\alpha-\beta)x-}\frac{(\alpha+2)(3+\gamma-\beta)x}{\gamma+3+(2+\alpha-\beta)x-}\cdots. \tag{27}$$

This is a new equality between continued fractions. One could get a newer result by proceeding as above but carrying the algebra two steps further and then using Euler's continued fraction. This is exactly what Perron first and independently Ramanujan did. If we take $x=-1$, (27) takes the neater form

$$\gamma+\frac{\beta(\gamma-\alpha)}{\gamma+1+}\frac{(\alpha+1)(\gamma+1-\beta)}{\gamma+\beta-\alpha+1+}\frac{(\alpha+2)(\gamma+2-\beta)}{\gamma+\beta-\alpha+1+}\cdots$$

$$=\gamma+\beta-\alpha-1+\frac{(\alpha+1)(\gamma+1-\beta)}{\gamma+\beta-\alpha-1+}\frac{(\alpha+2)(\gamma+2-\beta)}{\gamma+\beta-\alpha-1+}\cdots. \tag{28}$$

This result was first proved by Perron ([9] First edition 1913, p. 223) as a consequence of a theorem of Muir. To identify (28) with Perron's statement, replace α,β,γ by $\alpha/c,\beta/c,\gamma/c$, $c>0$ respectively and put

$$\alpha=a+b,\quad \beta=h+b+c,\quad \gamma=h+a+c. \tag{29}$$

$$2h+c+\frac{(a+c)^2-b^2}{2h+c+}\frac{(a+2c)^2-b^2}{2h+c+}\cdots$$

$$=h+a+c+\frac{(h+c)^2-b^2}{h+a+2c+}\frac{(a+c)^2-b^2}{2h+3c+}\frac{(a+2c)^2-b^2}{2h+3c+}\cdots. \tag{30}$$

This result can be generalized leading to a theorem of Ramanujan (Vol. 2, p. 342). We mention, in passing, that for convergence

$$c\geqslant 0,\quad 2h+c>0,\quad a+c\geqslant 0,\quad (a+c)^2>b^2>-\infty. \tag{31}$$

Let us denote the left side of (30) by $\varphi(h,a)$. Then $\varphi(h,a)$ consists of positive terms. Furthermore

$$\varphi(h,a)=h+a+c+\frac{(h+c)^2-b^2}{h+a+2c+}\frac{(a+c)^2-b^2}{\varphi(h+c,a+c)}. \tag{32}$$

Since $\varphi(h,a)$ converges for (31), we have, by induction

$$\varphi(h,a)=h+a+c+\frac{(h+c)^2-b^2}{h+a+2c+}\frac{(a+c)^2-b^2}{h+a+3c+}\cdots\frac{(h+nc)^2-b^2}{h+a+2nc+}$$

$$\frac{(a+nc)^2-b^2}{h+a+(2n+1)c+\cdots}. \tag{33}$$

As mentioned above Ramanujan has stated this in Vol. 2, p. 342. In order to identify it with Ramanujan's statement, put

$$c=2,\quad h+1=x,\quad a+1=y,\quad b^2=-N. \tag{34}$$

Then

$$x+\frac{(y+1)^2+N}{2x+}\frac{(y+3)^2+N}{2x+}\frac{(y+5)^2+N}{2x+}\cdots$$

$$=y+\frac{(x+1)^2+N}{x+y+2+}\frac{(y+1)^2+N}{x+y+4+}\frac{(x+3)^2+N}{x+y+6+}\frac{(y+3)^2+N}{x+y+8+}\cdots. \tag{35}$$

We make one last application of a three-term relation. Clearly we have

$$\frac{\gamma f(\alpha,\beta;\gamma,-1)}{f(\alpha+1,\beta;\gamma+1,-1)}=\frac{\gamma f(\alpha,\beta-1;\gamma,-1)}{f(\alpha+1,\beta;\gamma+1,-1)}-\alpha$$

so that on substitution of (29) for α, β, γ,

$$G(h,a)=h+\frac{c}{2}+\frac{(a+c)^2-b^2}{2h+c+}\frac{(a+2c)^2-b^2}{2h+c+}\cdots$$

$$=(a+h+c)\frac{f\left(\frac{a+b}{c},\frac{h+b}{c};\frac{h+a+c}{c},-1\right)}{f\left(\frac{a+b+c}{c},\frac{h+b+c}{c};\frac{h+a+2c}{c},-1\right)}$$

$$\left(\qquad\qquad\frac{c}{}\right)$$

Since the hypergeometric series is symmetric in the first two variables and hence in a and h, we get

$$G(h, a) = G(a, h)$$

and therefore

$$G(h,a) = h + \frac{c}{2} + \frac{(a+c)^2 - b^2}{2h + c +} \frac{(a+2c)^2 - b^2}{2h + c +} \cdots$$

$$= a + \frac{c}{2} + \frac{(h+c)^2 - b^2}{2a + c +} \frac{(h+2c)^2 - b^2}{2a + c +} \cdots = G(a, h). \tag{36}$$

This result which is equivalent to Ramanujan's result given below was first discovered and proved by Perron in 1913 (First edition, p. 228). He used Muir's method. We have obtained it as part of results relating to three-term relations for hypergeometric series. If we use the values of c, x, y, N given earlier we get

$$x + \frac{(y+1)^2 + N}{2x +} \frac{(y+3)^2 + N}{2x +} \frac{(y+5)^2 + N}{2x +} \cdots$$

$$= y + \frac{(x+1)^2 + N}{2y +} \frac{(x+3)^2 + N}{2y +} \frac{(x+5)^2 + N}{2y +} \cdots. \tag{37}$$

This formula was communicated by Ramanujan to Hardy in his second letter of February 27, 1913. It is given on page 190 of Volume 1 and on page 148, Entry 27 and page 342 of Volume 2.

5. Continued fractions of Ramanujan

Chapters XII, XIII and XIV of Notebook 1 are devoted to hypergeometric series and continued fractions. One looks in vain in these and other chapters of Volume 1, for results on q-series. However on the left hand side pages 124, 134, 146, 158, 160 (in the pagination of Notebook I [12]) there are a number of results on basic hypergeometric series and continued fractions associated to them.

Heine's work [8] is mentioned in Carr's book only in the section on references at the end of that book. Heine's generalization of Gauss' continued fraction is given as an exercise in Chrystal's Algebra. Ramanujan had perhaps seen Chrystal's book which was widely used in colleges in India. In view of the results mentioned above in the pages of Volume 1, it seems that Ramanujan had thought of q-generalizations of results on hypergeometric series and continued fractions. Chapter XVI of Notebook II, perhaps one of the best chapters in the Notebook shows some aspects of these generalizations.

Set q be a parameter $|q| < 1$ and

$$(a, q)_\infty = (1-a)(1-aq)\cdots = \prod_{n=0}^{\infty} (1 - aq^n)$$

and

$$(a, q)_n = (a, q)_\infty / (aq^n, q)_\infty,$$

so that for n a positive integer

$$(a, q)_n = (1 - a)(1 - aq)\cdots(1 - aq^{n-1}), \quad (a, q)_0 = 1.$$

Heines' basic hypergeometric series is defined by

$$\varphi(\alpha, \beta; \gamma, q, x) = \sum_{m=0}^{\infty} \frac{(\alpha, q)_m (\beta, q)_m}{(q, q)_m (\gamma, q)_m} \cdot x^m$$

and is convergent for $|x| < 1$. If we define two series $\varphi(\alpha, \beta; \gamma, q, x)$ and $\varphi(\alpha', \beta'; \gamma', q, x)$ to be contiguous if

$$\alpha/\alpha', \quad \beta/\beta', \quad \gamma/\gamma' \tag{38}$$

are integral powers of q, then Heine showed that any three contiguous functions satisfy a linear relation. He obtained the analogues of all the three-term relations of Gauss for the ordinary hypergeometric series. In view of Heine's identity

$$\varphi(\alpha, \beta; \gamma, q, x) - \varphi(\alpha, \beta; \gamma, q, qx) = \frac{(1 - \alpha)(1 - \beta)x}{1 - \gamma} \varphi(\alpha q, \beta q; \gamma q, x) \tag{39}$$

we may include change of x by powers of q in our definition of contiguous functions.

If we take q^2 instead of q for the step, then

$$(\alpha, q^2)_m (\beta, q^2)_m = (1 - \alpha)(1 - \alpha q^2)\cdots(1 - \alpha q^{2m-2})$$
$$\times (1 - \beta)(1 - \beta q^2)\cdots(1 - \beta q^{2m-2})$$

and hence

$$(\alpha, q^2)_m (\alpha q, q^2)_m = (\alpha, q)_{2m}.$$

Therefore

$$\varphi(\alpha, \alpha q; q, q^2, x^2) = \sum_{m=0}^{\infty} \frac{(\alpha, q)_{2m}}{(q, q)_{2m}} x^{2m}.$$

The q-binomial theorem states

$$1 + \frac{1 - \alpha}{1 - q} x + \frac{(1 - \alpha)(1 - \alpha q)}{(1 - q)(1 - q^2)} x^2 + \cdots = \frac{(\alpha x, q)_\infty}{(x, q)_\infty}$$

and hence

$$\varphi(\alpha q, \alpha; q, q^2, x^2) = \frac{1}{2}\left(\frac{(\alpha x, q)_\infty}{(x, q)_\infty} + \frac{(-\alpha x, q)_\infty}{(-x, q)_\infty}\right)$$

and

$$\frac{(1 - \alpha)x}{1 - q} \varphi(\alpha q, \alpha q^2; q^3, q^2, x^2) = \frac{1}{2}\left(\frac{(\alpha x, q)_\infty}{(x, q)_\infty} - \frac{(-\alpha x, q)_\infty}{(-x, q)_\infty}\right).$$

Heine's generalization of Gauss' continued fraction states

$$\frac{\varphi(\alpha, \beta q; \gamma q, q, x)}{\varphi(\alpha, \beta; \gamma, q, x)} = \frac{1}{1 -} \frac{\beta_1}{1 -} \frac{\beta_2}{1 -} \cdots,$$

where

$$\beta_{2r}=\frac{(1-\beta q^r)(1-\gamma q^r/\alpha)}{(1-\gamma q^{2r-1})(1-\gamma q^{2r})}\alpha x q^{r-1}, \quad r\geqslant 1$$

$$\beta_{2r+1}=\frac{(1-\alpha q^r)(1-\gamma q^r/\beta)}{(1-\gamma q^{2r})(1-\gamma q^{2r+1})}\beta x q^r, \quad r\geqslant 0.$$

We then have Ramanujan's result (Chapter XVI, Vol. 2, Entry 11)

$$\frac{a-b}{1-q+}\frac{(a-bq)(aq-b)}{1-q^3+}\frac{(a-bq^3)(aq^3-b)}{1-q^5+}\cdots$$

$$=\frac{(b,q)_\infty(-a,q)_\infty-(-b,q)_\infty(a,q)_\infty}{(b,q)_\infty(-a,q)_\infty+(-b,q)_\infty(a,q)_\infty}. \tag{40}$$

Ramanujan obtained a q-generalization of Euler's continued fraction from the three-term relation

$$\varphi(\alpha,\beta;\gamma,q,x)=\left(1+\frac{\beta-\alpha q}{q(1-\gamma)}x\right)\varphi(\alpha q,\beta;\gamma q,q,x)-\frac{(1-\alpha q)(\beta-\gamma q)x}{q(1-\gamma)(1-\gamma q)}$$

$$\times\,\varphi(\alpha q^2,\beta;\gamma q^2,q,x), \tag{41}$$

namely

$$\frac{\varphi(\alpha q,\beta;\gamma q,q,x)}{\varphi(\alpha,\beta;\gamma,q,x)}=\frac{q(1-\gamma)}{q(1-\gamma)+(\beta-\alpha q)x+}\frac{(1-\alpha q)(\gamma q-\beta)xq}{q(1-\gamma q)+(\beta-\alpha q^2)x+}$$

$$\frac{(1-\alpha q^2)(\gamma q^2-\beta)xq}{q(1-\gamma q^2)+(\beta-\alpha q^3)x+}\cdots \tag{42}$$

If $x=-q/\alpha$, then q-analogue of Kummer's theorem can be applied to evaluate $\varphi(\alpha,\beta;\gamma,q,-q/\alpha)$ provided α,β,γ satisfy some conditions. The q-Kummer theorem was proved by Daum. A simple proof based on the q-binomial theorem was given by G E Andrews [2].

If we put

$$\beta q=\gamma\alpha, \quad x=-q/\alpha \tag{43}$$

then

$$\varphi(\alpha,\beta;\gamma,q,-q/\alpha)=\frac{(\beta q,q^2)_\infty(-q,q)_\infty\left(\frac{\beta q^2}{\alpha^2},q^2\right)_\infty}{\left(\frac{\beta q^2}{\alpha},q\right)_\infty(-q/\alpha,q)_\infty}. \tag{44}$$

We apply this to the left side of equation (42). The denominator is easily evaluated by (44). In order to evaluate the numerator we use the three-term relations

$$\varphi(\alpha,\beta;\gamma,q,x)=\varphi(\alpha q,\beta;\gamma q,q,x)-\frac{\alpha x(1-\beta)(1-\gamma/\alpha)}{(1-\gamma)(1-\gamma q)}\varphi(\alpha q,\beta q;\gamma q^2,q,x)$$

$$=\varphi(\alpha,\beta q;\gamma q,q,x)-\frac{\beta x(1-\alpha)(1-\gamma/\beta)}{(1-\gamma)(1-\gamma q)}\varphi(\alpha q,\beta q;\gamma q^2,q,x).$$

the main difficulty is due to the fact that $x = -q/\alpha$ depends on α and is not independent of α, β, γ as in the case of ordinary hypergeometric series.) We thus obtain

$$\frac{\varphi(\alpha q, \beta; \gamma q, q, -q/\alpha)}{\varphi(\alpha, \beta; \gamma, q, -q/\alpha)}$$

$$= \frac{(\alpha-\beta q)(\beta-\alpha)}{\beta(1-\alpha)(\alpha-q)} + \frac{\alpha(\alpha-\beta q)}{\beta(1-\alpha)(\alpha-q)} \cdot \frac{(\beta, q^2)_\infty \left(\frac{\beta q}{\alpha^2}, q^2\right)_\infty}{\left(\frac{\beta q^2}{\alpha^2}, q^2\right)_\infty (\beta q, q^2)_\infty}. \tag{45}$$

Ramanujan obtains a symmetric relation by taking

$$\alpha = aq/b, \quad \beta = a^2 q.$$

Thus

$$\frac{1}{1-ab} + \frac{(a-bq)(b-aq)}{(1-ab)(1+q^2)} + \frac{(a-bq^3)(b-aq^3)}{(1-ab)(1+q)^4} + \frac{(a-bq^5)(b-aq^5)}{(1-ab)(1+q^6)} + \cdots$$

$$= \frac{(a^2q^3, q^4)_\infty (b^2q^3, q^4)_\infty}{(a^2q, q^4)_\infty (b^2q, q^4)_\infty}. \tag{46}$$

Compare this with (25) using q-gamma functions of Jackson (see Askey [4]).

One might also consider the case

$$\beta = \gamma\alpha \tag{47}$$

one would obtain an analogue of (23). One would have to use (39) in order to evaluate the various hypergeometric series. We shall not proceed with this further.

6. Generalized Eisenstein fraction

Consider now the following identity due to Ramanujan stated as Entry 9 in Chapter XVI of Volume 2 of the Notebooks. It is

$$(-bq, q)_\infty \cdot \sum_{m=0}^{\infty} \frac{\lambda^m q^{m^2}}{(q, q)_m (-bq, q)_m}$$

$$= \sum_{m=0}^{\infty} \frac{(b+\lambda)(b+\lambda q)\cdots(b+\lambda q^{m-1}) q^{(m(m+1)/2)}}{(q, q)_m}. \tag{48}$$

This can be proved in several ways. It is obvious that each side is a limiting case of a basic hypergeometric series.

Let $h(b, \lambda)$ denote the right side of (48). Then

$$h(b, \lambda) = \lim_{\substack{a\to 0 \\ c\to 0}} \varphi\left(-\frac{\lambda}{b}, -\frac{q}{c}; -aq, q, bc\right) \tag{49}$$

as can be easily verified. We now consider the Gauss–Heine continued fractions for

$$\frac{\varphi(\alpha, \beta q; \gamma q, q, x)}{\varphi(\alpha, \beta; \gamma, q, x)} \quad \text{and} \quad \frac{\varphi(\alpha q, \beta; \gamma q, q, x)}{\varphi(\alpha, \beta; \gamma, q, x)}$$

with

$$\alpha = -\lambda/b, \quad \beta = -q/c, \quad \gamma = -aq, \quad x = bc \tag{50}$$

and take limits as $c \to 0$, $a \to 0$. We will then have continued fractions for

$$\frac{h(bq, \lambda q)}{h(b, \lambda)} \quad \text{and} \quad \frac{h(b, \lambda q)}{h(b, \lambda)}. \tag{51}$$

We take the Gauss–Heine continued fraction

$$\frac{\varphi(\alpha, \beta q; \gamma q, q, x)}{\varphi(\alpha, \beta; \gamma, q, x)} = \frac{1}{1-} \frac{\beta_1}{1-} \frac{\beta_2}{1-} \cdots$$

where

$$\beta_{2r} = \frac{(1 - \beta q^r)(\alpha - \gamma q^r) q^{r-1} x}{(1 - \gamma q^{2r-1})(1 - \gamma q^{2r})}, \qquad r \geqslant 1$$

$$\beta_{2r+1} = \frac{(1 - \alpha q^r)(\beta - \gamma q^r) q^r x}{(1 - \gamma q^{2r})(1 - \gamma q^{2r+1})}, \qquad r \geqslant 0$$

substitute from (50), take limits as $c \to 0$, $a \to 0$ and use Satz 3.10, P112 in Perron [9]. We obtain

$$\lim \beta_{2r} = -\lambda q^{2r}, \quad \lim \beta_{2r+1} = -q^{r+1}(b + \lambda q^r)$$

and hence

$$\frac{h(bq, \lambda q)}{h(b, \lambda)} = \frac{1}{1+} \frac{q(b+\lambda)}{1+} \frac{\lambda q^2}{1+} \frac{q^2(b+\lambda q)}{1+} \frac{\lambda q^4}{1+} \cdots . \tag{52}$$

In a similar way

$$\frac{h(b, \lambda q)}{h(b, \lambda)} = \frac{1}{1+} \frac{\lambda q}{1+} \frac{q(b+\lambda q)}{1+} \frac{\lambda q^3}{1+} \frac{q^2(b+\lambda q^2)}{1+} \cdots . \tag{53}$$

We now take the left side of (48) and call it $g(b, \lambda)$. It is clear that

$$g(b, \lambda) = \lim_{\substack{a \to 0 \\ c \to 0}} (-bq; q)_\infty \, \varphi\left(-\frac{\lambda q}{c}, -\frac{1}{a}; -bq, q, ac\right).$$

We now take the q-Euler continued fraction as given in (42) and substitute

$$\alpha = -\lambda q/c, \quad \beta = -1/a, \quad \gamma = -bq, \quad x = ac. \tag{54}$$

If we take limits as $c \to 0$, $a \to 0$, then

$$g(b, \lambda) = (1 + bq) \cdot g(bq, \lambda q) + \lambda q \cdot g(bq^2, \lambda q^2) \tag{55}$$

$$\frac{g(b,\lambda)}{g(b,\lambda)} = \frac{1}{1+bq+}\,\frac{\lambda q}{1+bq^2+}\,\frac{\lambda q^2}{1+bq^3+}\cdots. \tag{56}$$

Since $h(b,\lambda) = g(b,\lambda)$ by (48), we have from (52) and (56)

$$\frac{1}{1+bq+}\,\frac{\lambda q}{1+bq^2+}\,\frac{\lambda q^2}{1+bq^3+}\cdots = \frac{1}{1+}\,\frac{q(b+\lambda)}{1+}\,\frac{\lambda q^2}{1+}\,\frac{q^2(b+\lambda q)}{1+}\cdots. \tag{57}$$

From (55) we have

$$g(b,\lambda q) = (1+bq)\cdot g(bq,\lambda q^2) + \lambda q^2 \cdot g(bq^2,\lambda q^3).$$

On the other hand one can prove easily that

$$g(b,\lambda) = g(b,\lambda q) + \lambda q g(bq,\lambda q^2).$$

From these two relations we have

$$\frac{g(b,\lambda q)}{g(b,q)} = \frac{h(b,\lambda q)}{h(b,q)} = \frac{1}{1+}\,\frac{\lambda q}{1+bq+}\,\frac{\lambda q^2}{1+bq^2+}\,\frac{\lambda q^3}{1+bq^3+}\cdots$$

$$= \frac{1}{1+}\,\frac{\lambda q}{1+}\,\frac{q(b+\lambda q)}{1+}\,\frac{\lambda q^3}{1+}\,\frac{q^2(b+\lambda q^2)}{1+}\cdots$$

$$= \sum_{m=0}^{\infty} \frac{\lambda^m \cdot q^{m^2+m}}{(q,q)_m(-bq,q)_m} \Big/ \sum_{m=0}^{\infty} \frac{\lambda^m q^{m^2}}{(q,q)_m(-bq,q)_m}. \tag{58}$$

The equality of the second and fourth results was stated by Ramanujan in his Notebook II, chapter XVI, Entry 15. If $b = 0$, it asserts the equality

$$\frac{1}{1+}\,\frac{\lambda q}{1+}\,\frac{\lambda q^2}{1+}\cdots = \sum_{0}^{\infty} \frac{\lambda^m q^{m^2+m}}{(q,q)_m} \Big/ \sum_{0}^{\infty} \frac{\lambda^m q^{m^2}}{(q,q)_m}, \tag{59}$$

which is already due to L J Rogers. It was also independently discovered by Issai Schur in 1917.

If $b = -\lambda$ then by definition of $h(b,\lambda)$, we have $h(-\lambda,\lambda) = 1$ and hence

$$1 - \lambda q + \lambda^2 q^3 - \lambda^3 q^6 + \lambda^4 q^{10} - \cdots = \frac{1}{1+}\,\frac{\lambda q}{1+}\,\frac{\lambda(q^2-q)}{1+}\,\frac{\lambda q^3}{1+}\,\frac{\lambda(q^4-q^2)}{1+}\cdots. \tag{60}$$

This is a result due originally to Eisenstein. It is also stated by Ramanujan as Entry 13 of chapter XVI, Volume 2.

The left side of (60) is what Rogers calls a "false theta function".

If we put q^2 for q and λq^{-1} for λ, then (60) gives

$$1 - \lambda q + \lambda^2 q^4 - \lambda^3 q^9 + \lambda^4 q^{16} - \cdots = \frac{1}{1+}\,\frac{\lambda q}{1+}\,\frac{\lambda q(1-q^2)}{1+}\,\frac{\lambda q^5}{1+}\cdots \tag{61}$$

a theorem also due to Eisenstein.

$$\frac{}{1+}\,\frac{}{1+}\,\frac{}{1+}\,\frac{}{1+}\,\frac{}{1+}\cdots$$

a *generalized Eisenstein continued fraction.*

7. Modular functions

There are several examples of generalized Eisenstein continued fraction in Ramanujan's Notebooks as well as in the 'Lost' Notebook. For example if $b = \lambda = 1$, we have ([ ] p. 277)

$$\sum_0^\infty \frac{q^{m^2}}{(q^2,q^2)_m} = \prod_{m=1}^\infty (1+q^{2m-1}) = \frac{\prod_1^\infty (1-q^{2(2m-1)})}{\prod_1^\infty (1-q^{2m-1})}$$

$$\sum_0^\infty \frac{q^{m^2+m}}{(q^2,q^2)_m} = \prod_1^\infty (1+q^{2m}).$$

If we put

$$q = \exp(\pi i\tau), \quad \tau = x+iy, \quad y>0$$

then with

$$\eta(\tau) = q^{1/12}\prod_1^\infty (1-q^{2m}),$$

we have

$$\frac{\eta(\tau/2)}{\eta(\tau)} = f_1(\tau) = q^{-1/24}\prod_1^\infty (1-q^{2m-1}).$$

We then have Ramanujan's result (chapter XIX, Entry 1, Vol. 2)

$$\frac{q^{1/8}}{1+}\,\frac{q}{1+}\,\frac{q+q^2}{1+}\,\frac{q^3}{1+}\cdots = \frac{q^{1/8}}{1+}\,\frac{q}{1+q+}\,\frac{q^2}{1+q^2+}\,\frac{q^3}{1+q^3+}\cdots = \frac{f_1(\tau)}{(f_1(2\tau))^2}. \tag{62}$$

The function $f_1(\tau)$ is a modular function due to Schläfli. It is remarkable that Ramanujan gives the correct power $q^{1/8}$ with which to multiply the continued fraction to make it into a modular function.

Ramanujan came across the modular function of Schläfli in his work on modular equations, singular moduli etc. If

$$\tau = iK'/K = \sqrt{-n}, \quad n>0$$

n is an even integer, then $f_1(\tau)$ can be evaluated. Further $f_1(2\sqrt{-n})$ can be easily evaluated using a nice lemma due to Ramanujan (Notebook I, p. 320). For example

if $n = 2$

$$\frac{\exp(-\pi/\sqrt{2})/8}{1+}\,\frac{\exp(-\pi\sqrt{2})}{1+}\,\frac{\exp(-\pi\sqrt{2})+\exp(-2\pi\sqrt{2})}{1+}\,\frac{\exp(-3\pi\sqrt{2})}{1+}\cdots$$

$$=\frac{(\sqrt{2}-1)^{1/4}}{\sqrt{2}}.$$

Our second example is also from chapter XIX of Volume 2 of the Notebooks. It states that

$$\frac{q^{1/2}}{1+q+}\,\frac{q^2}{1+q^3+}\,\frac{q^4}{1+q^5+}\cdots = q^{1/2}\prod_1^\infty \frac{(1-q^{8m-1})(1-q^{8m-7})}{(1-q^{8m-3})(1-q^{8m-5})}. \tag{63}$$

The factor $q^{1/2}$ makes the right side a modular function. If in (57) we put q^2 for q, $\lambda = 1$ and $b = q^{-1}$ we see that

$$\frac{q^{1/2}}{1+}\,\frac{q+q^2}{1+}\,\frac{q^4}{1+}\,\frac{q^3+q^6}{1+}\cdots = q^{1/2}\prod_1^\infty \frac{(1-q^{8m-1})(1-q^{8m-7})}{(1-q^{8m-3})(1-q^{8m-5})} \tag{64}$$

a result obtained by Selberg [14]. From the definition of $h(b, \lambda)$, (63) and (64) are equal to

$$q^{1/2}\sum_{m=0}^{\infty}\frac{(-q,q^2)_m q^{m^2+2m}}{(q^2,q^2)_m}\Bigg/\sum_{m=0}^{\infty}\frac{(-q,q^2)_m\cdot q^{m^2}}{(q^2,q^2)_m}. \tag{65}$$

The infinite product for (65) was also proved by Andrews [2].

In his Notebooks Ramanujan has explicitly given an expression for (64) and (65) in terms of theta functions which exhibits it as a modular function.

8. The general continued fraction

A more general continued fraction was stated by Ramanujan in the 'Lost' Notebook [13]. He considers the function

$$G(a,\lambda) = G(a,\lambda,b,q) = \sum_{m=0}^{\infty}\frac{(\alpha+\lambda)(a+\lambda q)\cdots(a+\lambda q^{m-1})q^{(m(m+1)/2)}}{(q,q)_m(-bq,q)_m},$$

and states the very interesting result

$$\frac{G(aq,\lambda q)}{G(a,\lambda)} = \frac{1}{1+}\,\frac{(a+\lambda)q}{1+}\,\frac{bq+\lambda q^2}{1+}\,\frac{aq^2+\lambda q^3}{1+}\,\frac{bq^2+\lambda q^4}{1+}\cdots. \tag{66}$$

The continued fractions mentioned earlier are special cases of (66).

In §2 we had given three continued fractions of which two are due to Euler and Gauss. We shall consider the q-analogue of the second result in (8). Let us observe that

$$\varphi\left(\frac{-\lambda}{a},\frac{-q}{c};-bq,q,ac\right) = \sum_{m=0}^{\infty}\frac{\left(\frac{-\lambda}{a},q\right)_m\left(\frac{-q}{c},q\right)_m}{(q,q)_m(-bq,q)_m}a^m c^m$$

so that

$$\lim_{c\to 0}\varphi\left(\frac{-\lambda}{a},\frac{-q}{c};-bq,q,ac\right)=G(a,\lambda,b,q).$$

We now have the following q-analogues of the two results in (9).

$$\begin{aligned}&\varphi(\alpha,\beta;\gamma,q,x)\\&\quad=\varphi(\alpha,\beta q;\gamma,q,x)-\frac{\beta x(1-\alpha)}{1-\gamma}\varphi(\alpha q,\beta q;\gamma q,q,x)\\&\quad=\frac{\beta-\gamma}{\beta(1-\gamma)}\varphi(\alpha q,\beta;\gamma q,q,x)+\frac{(1-\beta)(\gamma-\alpha\beta x)}{\beta(1-\gamma)}\varphi(\alpha q,\beta q;\gamma q,q,x).\end{aligned}\tag{67}$$

The first of these two formulae is already in Heine's paper [8]. As for the second, eliminate $\varphi(\alpha q^2,\beta q;\gamma q^2,q,x)$ from the following two results of Heine:

$$\left.\begin{aligned}&\varphi(\alpha q,\beta;\gamma q,q,x)-\varphi(\gamma q,\beta;\gamma,q,x)\\&\quad=-\frac{\gamma x(1-\alpha q)(1-\beta)}{(1-\gamma)(1-\gamma q)}\varphi(\alpha q^2,\beta q;\gamma q^2,q,x)\end{aligned}\right\}$$

$$\left.\begin{aligned}&\varphi(\alpha q,\beta q;\gamma q,q,x)-\varphi(\alpha q,\beta;\gamma,q,x)\\&\quad=\frac{\beta x(1-\alpha q)(1-\gamma/\beta)}{(1-\gamma)(1-\gamma q)}\varphi(\alpha q^2,\beta q;\gamma q^2,q,x)\end{aligned}\right\}$$

to obtain

$$\begin{aligned}&(\beta-\gamma)(\varphi(\alpha q,\beta;\gamma q,q,x)-\varphi(\alpha q,\beta;\gamma,q,x))\\&\quad+\gamma(1-\beta)(\varphi(\alpha q,\beta q;\gamma q,q,x)-\varphi(\alpha q,\beta;\gamma,q,x))=0.\end{aligned}$$

Now substitute for $\varphi(\alpha q,\beta;\gamma,q,x)$ from Heine's result

$$\varphi(\alpha q,\beta;\gamma,q,x)=\varphi(\alpha,\beta;\gamma,q,x)+\frac{\alpha x(1-\beta)}{1-\gamma}\varphi(\alpha q,\beta q;\gamma q,q,x),$$

we then obtain the second result in (67).

We now use the two three-term relations alternately and obtain the continued fraction

$$\begin{aligned}&\frac{\varphi(\alpha,\beta q;\gamma,q,x)}{\varphi(\alpha,\beta;q,x)}\\&\quad=\frac{1}{1-}\frac{\beta^2qx(1-\alpha)}{\beta q-\gamma+}\frac{(1-\beta q)(\gamma-x\alpha\beta q)}{1-}\frac{\beta^2q^3x(1-\alpha q)}{\beta q^2-\gamma q+}\cdots.\end{aligned}\tag{68}$$

Let us now make the substitution

$$\alpha=\frac{-\lambda}{a},\quad\beta=\frac{-q}{c},\quad\gamma=-bq,\quad x=ac$$

and take the limit as $c\to 0$. Then by a theorem of Perron we obtain (66).

We now again take two more three-term relations

$$\varphi(\alpha,\beta;\gamma,q,x)$$

$$=\varphi(\alpha,\beta q;\gamma,q,x)-\frac{\beta x(1-\alpha)}{1-\gamma}\varphi(\alpha q,\beta q;\gamma q,q,x)$$

$$=\left(1+\frac{(\beta-\alpha q)x}{q(1-\gamma)}\right)\varphi(\alpha q,\beta;\gamma q,q,x)-\frac{(1-\alpha q)(\beta-\gamma q)x}{q(1-\gamma)(1-\gamma q)}$$

$$\times\varphi(\alpha q^2,\beta;\gamma q^2,q,x).$$

The first relation is the same as that in (67) and the second relation is the same as (41). In the first place we have

$$\frac{\varphi(\alpha,\beta;\gamma,q,x)}{\varphi(\alpha,\beta q;\gamma,q,x)}=1-\frac{\beta x(1-\alpha)}{1-\gamma}\left(\frac{\varphi(\alpha,\beta q;\gamma,q,x)}{\varphi(\alpha q,\beta q;\gamma q,q,x)}\right)^{-1}. \tag{69}$$

For the ratio of the basic hypergeometric series on the right of (69) we use the continued fraction (42) after changing β into βq in (42). We have

$$\frac{\varphi(\alpha,\beta q;\gamma,q,x)}{\varphi(\alpha,\beta;\gamma,q,x)}$$

$$=\frac{1}{1-}\frac{\beta(1-\alpha)xq}{q(1-\gamma)+(\beta-\alpha)xq-}\frac{(1-\alpha q)(\beta q-\gamma q)xq}{q(1-\gamma q)+(\beta q-\gamma q^2)x-}\cdots. \tag{70}$$

Inserting the values of α,β,γ,x as given above and taking the limit when $c\to 0$ we have

$$\frac{G(aq,\lambda q)}{G(a,\lambda)}=\frac{1}{1+}\frac{q(a+\lambda)}{1-aq+bq+}\frac{q(a+\lambda q)}{1-aq+bq^2+}\frac{q(a+\lambda q^2)}{1-aq+bq^3+}\cdots. \tag{71}$$

It is clear that this is a generalization of (58). One can also obtain a generalization of (57).

The interesting problem now is to find values of a,b,λ for which $G(aq,\lambda q)/G(a,\lambda)$ is an infinite product. Ramanujan put q^2 for q and aq^{-1} for a and $\lambda=1$ to obtain

$$R(a,b,q)=\frac{1}{1+}\frac{aq+q^2}{1+}\frac{bq^2+q^4}{1+}\frac{aq^3+q^6}{1+}\cdots$$

$$=\frac{\sum_{m=0}^{\infty}\frac{(a+q)(a+q^3)\cdots(a+q^{2m-1})q^{m^2+2m}}{(q^2,q^2)_m(-bq^2,q^2)_m}}{\sum_{m=0}^{\infty}\frac{(a+q)(a+q^3)\cdots(a+q^{2m-1})q^{m^2}}{(q^2,q^2)_m(-bq^2,q^2)_m}}. \tag{72}$$

Ramanujan now considers the 9 cases.

$$a=0,\pm 1,\quad b=0,\pm 1. \tag{73}$$

Precisely these 9 cases were independently considered by Selberg [14]. Selberg, Andrews and Ramanujan found four cases in which the right side of (72) is a product.

One of these is

$$q^{1/5}R(0,0,\sqrt{q}) = \frac{q^{1/5}}{1+}\frac{q}{1+}\frac{q^2}{1+}\cdots = q^{1/5}\prod_{m=0}^{\infty}\frac{(1-q^{5m+1})(1-q^{5m+4})}{(1-q^{5m+2})(1-q^{5m+3})}$$

which Ramanujan discussed extensively in the Notebooks and the 'Lost' Notebook. The other which Ramanujan discussed at length in the unpublished manuscripts (now published [13]) is

$$q^{1/3}R(1,1,q) = \frac{q^{1/3}}{1+}\frac{q+q^2}{1+}\frac{q^2+q^4}{1+}\cdots = \frac{f_1(\tau)}{(f_1(3\tau))^3}. \tag{74}$$

Actually a result equivalent to this was first proved by G N Watson [15] where he used his q-generalization of Whipple's theorem on the ${}_7F_6$. Selberg's method, as mentioned earlier, is elementary. Andrews uses some theorems of Slater.

From the form of the right side in (74) it follows that one can evaluate the continued fraction on the left of (74) for $\tau = i\sqrt{n}$, where n is even idoneal number of Euler. Ramanujan in his Notebook I, p. 318 has given a formula for $f_1(3\sqrt{-n})$ in terms of $f_1(\sqrt{-n})$. This shows that the continued fraction on the left of (74) can be evaluated for an infinity of $3^k\sqrt{-n}, k$ any rational integer. Ramanujan himself stated [12] the result for $n = 10$.

References

[1] Adiga C, Bhargava S, Berndt B C and Watson G N, Chapter XVI of Ramanujan's Notebook II. *Mem. Am. Math. Soc.* **53** (1985) pp. 1–85

[2] Andrews G E, On the q-analog of Kummer's theorem and applications, *Duke Math. J.* **40** (1973) 525–528

[3] Andrews G E, An introduction to Ramanujan's Lost Notebook, *Am. Math. Mon.* **86** (1979) 89–108

[4] Askey R, The q-gamma and the q-beta functions, *Appl. Anal.* **8** (1978) 125–141

[5] Berndt B C, Lamphere R L and Wilson B M, Chapter 12 of Ramanujan's second Notebook; continued fractions, *Rocky Mountain J. Math.* **15** (1985) 235–310

[6] Gauss C F, Gesammelte Werke, Bd III, Göttingen (1876) 123–162

[7] Hardy G H and Wright E M, *An introduction to the theory of numbers* (Oxford: University Press) (1960)

[8] Heine E, Untersuchunger über die Reihe, *J. für Math.* **34** (1847) 285–328

[9] Perron O, *Die Lehre von den Kettenbrüchen* (Erste Auflage 1913; Dritte Verbesserte Auflage B G Teubner Stuttgart 1957)

[10] Ramanathan K G, Remarks on some series considered by Ramanujan, *J. Indian Math. Soc.* **46** (1982) 107–136

[11] Ramanathan K G, Ramanujan's continued fraction, *Indian J. Pure Appl. Math.* **16** (1985) 695–724

[12] Ramanujan S, *Notebooks* (Bombay: Tata Institute of Fundamental Research) Vol. 1 and 2 (1957)

[13] Ramanujan S, *The lost notebook and other unpublished papers* (New Delhi: Narosa Publishing House) (1987)

[14] Selberg A, Über einige arithmetische Identitäten, *Avh. Nor. Vidensk.-Akad. Oslo, Mat. Naturvidensk. Kl.* (1936) No. 8, pp. 1–23

[15] Watson G N, Theorems stated by Ramanujan IX: Two theorems on continued fractions, *J. London Math. Soc.* **4** (1929) 231–237

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 297–303.
© Printed in India.

Multiplicative properties of the partition function

A SCHINZEL and E WIRSING*
Mathematics Institute PAN, P O Box 137, 00–950 Warszawa, Poland
* Abteilung Mathematik II, Universität Ulm, Oberer Eselsberg, 7900 Ulm, FRG

Abstract. A lower bound for the number of multiplicatively independent values of $p(n)$ for $N \leqslant n < N + R$ is given. The proof depends on the Hardy-Ramanujan formula and is of an elementary nature.

Keywords. Partition function; Hardy-Ramanujan formula; multiplicative independence of integers.

1. Introduction

P Erdös and A Ivić [1] in their study of the number of non-isomorphic Abelian groups of a given order needed a lower estimate for the number $m(N)$ of multiplicatively independent values of the partition function $p(n)$ in $1 \leqslant n \leqslant N$. The first named author has proved (see [1], lemma 2) that, denoting the number of prime devisors of n by $\omega(n)$, one has

$$\omega\left(\prod_{n=1}^{N} p(n)\right) \to \infty,$$

whence $m(N) \to \infty$, as $N \to \infty$.

In the present paper we give an explicit estimate for $m(N)$, at the same time eliminating from the proof the appeal to "linear forms in logarithms". What we actually treat is the number $m(N, N+R)$ of multiplicatively independent values of $p(n)$ in $N \leqslant n < N + R$, where R is relatively small compared to N.

2. Theorem

There is an N_0 such that

$$m(N, N+R) \geqslant R \frac{\log N - \log R}{\frac{3}{2}\log N + R \log 2}$$

for $N \geqslant N_0$ and all $R \in \mathbb{N}$.

The same lower bound applies to

$$\omega\left(\prod_{N\leqslant n<N+R} p(n)\right)$$

which is, of course, $\geqslant m(N, N+R)$.

It will be seen that, given N, our bound decreases as a function of R for $R \geqslant \log^2 N$, more precisely if $R \log 2 > 2/3 \log N(\log N - 1 - \log R)$. Thus in the proof and in applications like corollary 2 below there is no need to consider larger R.

COROLLARY 1

$$m(N, N+R) \geqslant (\tfrac{2}{3} - o(1))R \quad \text{if } R = o(\log N) \text{ as } N \to \infty.$$

COROLLARY 2

$$m(N, N+R) \geqslant \left(\frac{1}{\log 2} - o(1)\right)\log N \quad \text{if } \frac{R}{\log N} \to \infty \text{ as } N \to \infty.$$

In particular we may state that

$$\omega\left(\prod_{1}^{N} p(n)\right) \geqslant m(N) \geqslant (1-\varepsilon)\frac{\log N}{\log 2} \quad \text{if } N \geqslant N_0(\varepsilon).$$

Concerning the paper of Erdös and Ivić we have

COROLLARY 3

Let $a(n)$ be the number of non-isomorphic Abelian groups of order n and $C(x)$ the number of distinct values of $a(n)$ for $n \leqslant x$. Then for every $\varepsilon > 0$ and $x \geqslant x_1(\varepsilon)$

$$\log C(x) \geqslant \frac{(\log\log x)^2}{\log 16 + \varepsilon}.$$

Similarly for the number $D(x)$ of distinct values $a(n) \leqslant x$ with any n one has, if $x \geqslant x_2(\varepsilon)$,

$$\log D(x) \geqslant \frac{(\log\log x)^2}{\log 4 + \varepsilon}.$$

Proof of corollary 3. Notation as in [1]. Our corollary 2 allows to pick $p(k_i)$ multiplicatively independent, $k_1, \ldots, k_t \leqslant \sqrt{\log x}$, with $t(\log 4 + \varepsilon) \sim \log\log x$. The construction gives $C(x) \geqslant r^t$ where $2rt \log(rt) \leqslant \sqrt{\log x}$. Here $r = [(\log x)^{1/2-\varepsilon}]$ is admissible if $x \geqslant x_1$, which gives our proposition.

For the estimate of $D(x)$ take $k_1, \ldots, k_t \leqslant \log x$ with $t(\log 2 + \varepsilon) \sim \log\log x$. Now $D(x) \geqslant r^t$ upon the condition that $\sum_i r \log p(k_i) \leqslant \log x$, which because of $\log p(k) \ll \sqrt{k} \leqslant \sqrt{\log x}$ is again satisfied by $r \sim (\log x)^{1/2-\varepsilon}$.

3. The proof uses the Hardy-Ramanujan formula for $p(n)$ (see (1) below) to construct a large number of distinct linear combinations of the numbers $\log p(n)$ with bounded integral coefficients. If, on the other hand, the dimension of this $\mathbb{Z}$-module were too

small it would contain too few elements with bounded height. This mechanism is rather unspecific. Thus the theorem as it stands applies to any function $q(n) = p(n) + O[\exp(c\sqrt{n})]$ where $c < \pi\sqrt{2/3}$, and similar results can be proved whenever an arithmetic function $q(n)$ allows an expansion

$$\log q(n) = a_0 n^{\alpha_0} + a_1 n^{\alpha_1} + \cdots + b \log n + \text{remainder},$$

where $a_0 > 0, \alpha_0 > 0, \alpha_0 \notin \mathbb{N}$, $\alpha_0 > \alpha_1 > \cdots, \alpha_i - \alpha_{i+1} \gg 1$, and where the remainder term is small enough. The factor 2/3 in corollary 2 would become $(\alpha_0 + 1)^{-1}$.

Lemma 1. Write Δ for the forward difference and put

$$\Delta_r := |\Delta^r \log p(N)|.$$

Then, as $N \to \infty$, we have

$$\Delta_r = c_2 r! \left| \binom{1/2}{r} \right| N^{1/2 - r}(1 + O(N^{-1/3}))$$

with some constant c_2, uniformly in $0 \leqslant r \leqslant N^{1/6}$.

Proof. The Hardy–Ramanujan formula (see [2]) gives

$$p(n) = c_1 f(n - \tfrac{1}{24}) + O[\exp(c_3\sqrt{n})], \tag{1}$$

where

$$f(x) := \left(\frac{1}{\sqrt{x}} \exp(c_2\sqrt{x}) \right)', \quad c_2 > c_3 > 0.$$

The actual values

$$\left(c_1 = \frac{1}{\pi\sqrt{8}}, c_2 = \pi\sqrt{2/3}, c_3 = \frac{c_2}{2} \right)$$

are mostly irrelevant for our purpose. Keeping the abbreviation $x = n - 1/24$ we find

$$p(n) = \frac{c_1}{2x}\left(c_2 - \frac{1}{\sqrt{x}} \right) \exp(c_2\sqrt{x}) + O[\exp(c_3\sqrt{x})]$$

$$= \frac{c_1}{2x}\left(c_2 - \frac{1}{\sqrt{x}} \right) \exp(c_2\sqrt{x})(1 + O[\exp(-c_4\sqrt{x})])$$

with some $c_4 > 0$. Therefore

$$\log p(n) = g(x) + O[\exp(-c_4\sqrt{n})],$$

where

$$g(x) = c_2\sqrt{x} + \log\frac{c_1 c_2}{2} + \log\left(1 - \frac{1}{c_2\sqrt{x}} \right) - \log x$$

—apart from the $\log x$ term—is a power series that converges for all large x,

$$g(x) = \sum_{i=-1}^{\infty} a_i x^{-i/2} - \log x.$$

Actually

$$a_{-1} = c_2, \quad |a_i| \leqslant c_2^{-i} \quad \text{for } i \geqslant 1.$$

The case $r = 0$ of the lemma is now obvious.

For $r \geqslant 1$ the generalized mean-value theorem gives

$$\Delta^r \log p(N) = g^{(r)}(\xi) + O(2^r \exp(-c_4\sqrt{N})),$$

where $N - \frac{1}{24} < \xi < N + r$. Hence for $r \geqslant 1$

$$\Delta^r \log p(N) = r! \sum_{\substack{i=-1 \\ i \neq 0}}^{\infty} a_i \binom{-i/2}{r} \xi^{-i/2-r} + (-1)^r (r-1)! \xi^{-r} + O(2^r \exp(-c_4\sqrt{N})).$$

If $i \geqslant 1$, $r \geqslant 1$, then

$$\binom{-(i+1)/2}{r}\binom{-i/2}{r}^{-1} = \prod_{j=0}^{r-1} \frac{\frac{i+1}{2} + j}{\frac{i}{2} + j}$$

$$< \prod_{0}^{r-1} \frac{\frac{i}{2} + 1 + j}{\frac{i}{2} + j} = 1 + \frac{2r}{i} \leqslant 3r.$$

Similarly

$$r!\left|\binom{-1/2}{r}\right|(r-1)!^{-1} \leqslant r, \quad (r-1)!\left(r!\left|\binom{1/2}{r}\right|\right)^{-1} \leqslant 4r.$$

Therefore

$$\Delta_r = c_2 r!\left|\binom{1/2}{r}\right| \xi^{1/2-r}\left(1 + \sum_{i=1}^{\infty} O\left(\left(\frac{4r}{c_2\sqrt{\xi}}\right)^i\right)\right) + O(2^r \exp(-c_4\sqrt{N}))$$

$$= c_2 r!\left|\binom{1/2}{r}\right| \xi^{1/2-r}\left(1 + O\left(\frac{r}{\sqrt{N}}\right)\right) + O(2^r \exp(-c_4\sqrt{N})).$$

We also have

$$\xi^{1/2-r} = (N + O(r))^{1/2-r} = N^{1/2-r}\left(1 + O\left(\frac{r}{N}\right)\right)^{1/2-r}$$

$$= N^{1/2-r}\left(1 + O\left(\frac{r^2}{N}\right)\right)$$

$$= N^{1/2-r}(1 + O(N^{-2/3}))$$

by our bound for r. Finally

$$2^r\left(r!\left|\binom{1/2}{r}\right|N^{1/2-r}\right)^{-1} \ll (2N)^r = \exp[o(\sqrt{N})],$$

whence altogether

$$\Delta_r = c_2 r!\left|\binom{1/2}{r}\right|N^{1/2-r}(1+O(N^{-1/3})+O[\exp(-c_4\sqrt{N}/2)])$$

for all $r \leqslant N^{1/6}$, which is the lemma.

Lemma 2. Let $R \leqslant N^{1/6}$ and $1 \leqslant r \leqslant R$. Then

$$\Delta_r/\Delta_{r-1} \leqslant R/N$$

provided that $N \geqslant N_0$. The N_0 does not depend on R.

Proof. Lemma 1 for $2 \leqslant r \leqslant N^{1/6}$ supplies

$$\frac{\Delta_r}{\Delta_{r-1}} = \frac{r-\frac{3}{2}}{N}(1+O(N^{-1/3}))$$

$$= \frac{r}{N} - \frac{3}{2N} + O\left(\frac{r}{N^{4/3}}\right) < \frac{r}{N} \leqslant \frac{R}{N}$$

if $N \geqslant N_0$, and similarly for $r = 1$.

Proof of the theorem

We assume, somewhat arbitrarily, $R \leqslant N^{1/6}$. This includes for large N the range $R \leqslant \log^2 N$ that by an earlier remark is relevant.

Consider now the numbers

$$\omega = \sum_{r=0}^{R-1} x_r\Delta_r, \quad \text{where } x_r \in \mathbb{N}_0, \quad x_r \leqslant \frac{N}{R} - 1.$$

They all are distinct because of

$$\sum_{r=s+1}^{R-1} x_r\Delta_r \leqslant \sum_{s+1}^{R-1}\left(\frac{N}{R}-1\right)\Delta_r \leqslant \sum_{s+1}^{R-1}(\Delta_{r-1}-\Delta_r) < \Delta_s.$$

The number A of the ω's is therefore

$$A = \left[\frac{N}{R}\right]^R > \left(\frac{N}{R}-1\right)^R = \left(\frac{N}{R}\right)^R\left(1-\frac{R}{N}\right)^R$$

$$\geqslant \left(\frac{N}{R}\right)^R\left(1+O\left(\frac{1}{\sqrt{N}}\right)\right)$$

as $N \to \infty$.

On the other hand

$$\Delta_r = \varepsilon_r \sum_{s=0}^{r} (-1)^s \binom{r}{s} \log p(N+s), \quad \varepsilon_r = \pm 1$$

implies that each ω is a linear combination over $\mathbb{Z}$ of the $\log p(n)$, $N \leqslant n < N+R$. If $q_1, \ldots, q_k$ denote the primes that make up the $p(N), \ldots, p(N+R-1)$,

$$p(n) = \prod_{j=1}^{k} q_j^{a_j(n)}, \quad a_j(n) \in \mathbb{N}_0,$$

say, then we obtain the representation

$$\omega = \sum_{j=1}^{k} y_j \log q_j$$

with

$$y_j := \sum_{0 \leqslant s \leqslant r < R} \varepsilon_r (-1)^s \binom{r}{s} x_r a_j(N+s).$$

Trivially $a_j(n) \leqslant (\log p(n))/\log 2$. Therefore, if N is large,

$$a_j(n) \leqslant c_2 \frac{\sqrt{n}}{\log 2},$$

$$|y_j| \leqslant \frac{c_2}{\log 2} \sqrt{N+R} \sum_{r=0}^{R-1} 2^r x_r$$

$$\leqslant \frac{c_2}{\log 2} \sqrt{N+R} \cdot 2^R \binom{N}{R-1}$$

$$\leqslant \frac{c_2}{\log 2} N^{3/2} \frac{2^R}{R}$$

for $1 \leqslant j \leqslant k$.

If now $m(N, N+R) =: l$ then the ω's are elements of an l-dimensional $\mathbb{Z}$-module. A suitable choice of l of the coordinates $y_j (j = 1, \ldots, k)$ will then determine the $k-l$ others. The number A of the ω's can therefore not exceed

$$\left(\frac{2c_2}{\log 2} N^{3/2} \frac{2^R}{R} + 1 \right)^l.$$

Consequently

$$\left(\frac{3c_2}{\log 2} N^{3/2} \frac{2^R}{R} \right)^l \geqslant \binom{N}{R}^R \left(1 + O\left(\frac{1}{\sqrt{N}} \right) \right). \tag{2}$$

Thus, if any $R_0 > 3c_2/\log 2$ and a suitable N_0 are chosen then for all $R \geqslant R_0$ and $N \geqslant N_0$

$$(2^R N^{3/2})^l \geqslant \binom{N}{R}^R \frac{R_0 \log 2}{3c_2} \left(1 + O\left(\frac{1}{\sqrt{N}} \right) \right) \geqslant \binom{N}{R}^R,$$

as claimed. For each of the remaining $R < R_0$, formula (2) implies $3l \geqslant 2R - \varepsilon$. and therefore $3l \geqslant 2R$, if N is large enough, hence again $(2^R N^{3/2})^l \geqslant (N/R)^R$.

References

[1] Erdös P and Ivič A, The distribution of values of a certain class of arithmetic functions at consecutive integers (to appear)

[2] Hardy G H and Ramanujan S, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.* **17** (1918) 75–115

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 305–312.
© Printed in India.

The states of the character ring of a compact group

V S VARADARAJAN
Department of Mathematics, University of California, Los Angeles, California 90024, USA

Abstract. Deligne's generalization of the Hadamard–Vallée Poussin method in classical number theory is formulated as the representability of certain states of the character ring of a compact group, and the determination of all the representable states is carried out.

Keywords. Compact group; character ring; Hadamard–Vallée Poussin method; Deligne's generalization.

1. Introduction

The aim of this note is to make a few simple remarks on Deligne's generalization of the well-known method of Hadamard–de la Vallée Poussin in classical number theory ([2], § 2; see also the nice exposition by Moreno [4]). The Hadamard–de la Vallée Poussin method, as treated by Mertens, permits one to prove that the Riemann Zeta function and other L-functions do not vanish on the line $\mathrm{Re}(s) = 1$ (see [1]). Deligne's generalization leads to similar non-vanishing results for the L-functions that arise in non-classical situations. One may view the essential point in the proof of Deligne's main lemma as the assertion that a certain state of the complex character ring of a compact group is defined by an invariant measure on the group. This approach raises the questions that are discussed here.

Let G be a locally compact group and let $R_{\mathbf{Z}}(G)$ be the ring of integral linear combinations of the irreducible finite dimensional unitary characters of G. Write $R(G) = \mathbf{C} \otimes R_{\mathbf{Z}}(G)$. $R_{\mathbf{Z}}(G)$ is canonically isomorphic to the Grothendieck ring of the virtual finite dimensional unitary representations of G; $R(G)$ is a commutative algebra over $\mathbf{C}$ with an involution $*\,(a \to a^{\mathrm{conj}})$. If G^B is the Bohr compactification of G, we have $R_{\mathbf{Z}}(G) \cong R_{\mathbf{Z}}(G^B)$ and $R(G) \cong R(G^B)$ canonically, so that one may always suppose G to be compact; we shall do so from now on. Then Deligne's generalization is a consequence of the following lemma (Lemma 2.1.5 of [2]):

Lemma 1. Let ν be an additive map of $R_{\mathbf{Z}}(G)$ into $\mathbf{Z}$ with the following properties.

(a) $\nu(1) = 1$; $\nu(\tau) \leqslant 0$ *for all irreducible* $\tau \neq 1$,
(b) $\nu(\tau^*) = \nu(\tau)$,
(c) $\nu(\tau\tau^*) \geqslant 0$ *for all* $\tau \in R_{\mathbf{Z}}(G)$.

Then $\nu(\tau) = 0$ for all irreducible τ, except possibly for a single $\tau = \tau_0$; such a τ_0 is necessarily of degree 1, $(\tau_0)^2 = 1$, and $\nu(\tau_0) = -1$.

* Research partially supported by NSF Grant 85-01742.

It is actually sufficient to require (c) only for unitary characters ξ, i.e., *actual*, not virtual characters ξ, but possibly reducible. Indeed, if this is so and $\xi \in R_{\mathbf{Z}}(G)$ is arbitrary, we can write $\xi = \xi^1 - \xi^2$ where ξ^1, ξ^2 are characters of actual representations ρ^1, ρ^2 with no common irreducible constituent; the trivial representation does not occur in $\rho^1 \otimes (\rho^2)^{\text{conj}}$ and $(\rho^1)^{\text{conj}} \otimes \rho^2$, so that, using (a), we have

$$\nu(\xi\xi^*) = \nu(\xi^1\xi^{1*}) + \nu(\xi^2\xi^{2*}) - \nu(\xi^1\xi^{2*}) - \nu(\xi^2\xi^{1*}) \geqslant 0.$$

For finite G the proof is as follows. Taking ξ to be the character of the regular representation and using τ to denote irreducible characters, we get

$$0 \leqslant 1 + \Sigma_{\tau \neq 1} \deg(\tau)\nu(\tau) = 1 - \Sigma_{\tau \neq 1} \deg(\tau)|\nu(\tau)|.$$

So either $\nu(\tau) = 0$ for all irreducible $\tau \neq 1$ or else $|\nu(\tau_0)| = 1$ for exactly one $\tau_0 \neq 1$ with $\nu(\tau_0) = -1$, $\deg(\tau_0) = 1$; τ_0 then has to be real so that $(\tau_0)^2 = 1$. If G is infinite, the regular representation is infinite dimensional and one will have to modify this argument. We extend ν linearly to $R(G)$, write ν again for this extension, and note that ν is a *state* of the $*$-algebra $R(G)$:

$$\nu(\xi\xi^*) \geqslant 0, \quad \xi \in R(G).$$

One would expect that the state ν is defined by an invariant probability measure $p = p\nu$ on G:

$$\nu(\xi) = \int_G \xi \, dp, \quad \xi \in R(G).$$

If we assume this, Deligne's argument may be understood as follows. For any invariant continuous function g let $g^\wedge$ denote its Fourier transform defined on the set of irreducible characters by

$$g^\wedge(\tau) = (g, \tau) = \int_G g\tau^* \, dx.$$

One has $(g_1 * g_2)^\wedge(\tau) = (g_1)^\wedge(\tau)(g_2)^\wedge(\tau)\deg(\tau)^{-1}$. Let k_1 be any invariant continuous function on G which is $\geqslant 0$, symmetric, i.e., $k_1(x) = k_1(x^{-1})$, and normalized by the condition $\int_G k_1 \, dx = 1$, and let $k = k_1 * k_1$. Then $(k_1)^\wedge$ is real and $k^\wedge = ((k_1)^\wedge)^2 \deg^{-1}$ is $\geqslant 0$. By the Peter–Weyl theorem, $\Sigma_\tau k^\wedge(\tau)\tau$ converges to k in $L^2(G)$. But,

$$\Sigma_\tau |k^\wedge(\tau)| \sup|\tau| \leqslant \Sigma_\tau k^\wedge(\tau)\deg(\tau) = \Sigma_\tau (k_1)^\wedge(\tau)^2 = \|k_1\|_2^2 < \infty$$

so that we actually have

$$\Sigma_\tau k^\wedge(\tau)\tau = k$$

in the topology of uniform convergence. Integrating this relation with respect to p we get

$$\Sigma_\tau k^\wedge(\tau)\nu(\tau) = \int_G k \, dp \geqslant 0.$$

Since $\int_G k\,dx = 1$ and $\nu(\tau) \leqslant 0$ for $\tau \neq 1$, we get, for any finite set F of such τ's,

$$1 - \Sigma_{\tau \in F} k\hat{}(\tau)|\nu(\tau)| \geqslant 0.$$

Let us now take $k_1 = k_{1n}$ where the supports of the k_{1n} decrease to (e). Then, as $n \to \infty$, $k_n\hat{}(t) \to \deg(\tau)$ for each τ, and so we get

$$1 - \Sigma_{\tau \in F}|\nu(\tau)|\deg(\tau) \geqslant 0.$$

Since F is arbitrary, we get

$$\Sigma_{\tau \neq 1}|\nu(\tau)|\deg(\tau) \leqslant 1,$$

and the rest of the argument is the same as in the finite case.

This leads us to ask if states of a commutative $*$-algebra, especially $R(G)$, have integral representations. We discuss briefly the notion of a state and its representability in §2. In §3 we shall determine which states of $R(G)$ are representable by invariant measures on G and complete the above argument by proving the representability of ν. We shall also give an example of a state of $R(\mathrm{SU}(2))$ which is not representable by an invariant measure on $\mathrm{SU}(2)$, but which is nevertheless representable by a measure in $\mathrm{SL}(2, \mathbf{C})$, and we shall formulate a general result for all compact Lie groups that subsumes this example. We also discuss briefly the case when one deals with compact groups that are not Lie.

The author is grateful to Robert Blattner for many interesting discussions on these questions.

2. Commutative $*$-algebras and their states

Let $\mathbf{A}$ be a commutative complex $*$-algebra, i.e. a commutative algebra with unit over the field $\mathbf{C}$ of complex numbers with an involution $*(a^{**} = a,\ 1^* = 1,\ (ab)^* = a^*b^*$, and $a \to a^*$ is conjugate linear). A linear map $\lambda(\mathbf{A} \to \mathbf{C})$ is a *state* if $\lambda(1) = 1$ and $\lambda(aa^*) \geqslant 0$ for all $a \in \mathbf{A}$. The notion of a state of course makes sense even if $\mathbf{A}$ is non-commutative; the terminology and motivation come from quantum mechanics. It is standard that $\lambda(a^*) = \lambda(a)^{\mathrm{conj}}$ and that $(a, b)_\lambda := \lambda(ab^*)$ is a non-negative definite Hermitian scalar product for $\mathbf{A}$. If $\mathbf{A}$ is a $\mathbf{C}*$-algebra, i.e. a Banach algebra such that $\|aa^*\| = \|a\|^2$ for all $a \in \mathbf{A}$, then $\mathbf{A}$ is isomorphic to the $\mathbf{C}*$-algebra of all complex valued continuous functions on the Gel'fand spectrum of $\mathbf{A}$; it is then easy to show that there is a natural one-one correspondence $\lambda \leftrightarrow p\lambda$ between states λ and probability measures $p\lambda$ on the Gel'fand spectrum given by $\lambda(a) = \int a\,dp\lambda (a \in \mathbf{A})$ [3]. However, as the example of $R(G)$ shows, one often has to work with $*$-algebras $\mathbf{A}$ that are neither complete nor even normed; and it is natural to ask how much of the above integral representation remains valid in the more general contexts.

Given $\mathbf{A}$ and a state λ on $\mathbf{A}$ let $N_\lambda = \{a | (a, b)\lambda = 0 \text{ for all } a \in \mathbf{A}\}$; then N_λ is an ideal in $\mathbf{A}$ and $(.,.)\lambda$ defines the structure of a pre-Hilbert space on $\mathbf{A}/N_\lambda$; let $\mathscr{H}_\lambda$ be the completion of $\mathbf{A}/N_\lambda = \mathscr{H}_\lambda{}^0$. For each $a \in \mathbf{A}$ multiplication by a defines a linear operator $\pi|(a)$ on $\mathscr{H}_\lambda{}^0$; the map $a \to \pi\lambda(a)$ is a $*$-representation and $\pi\lambda(a^*)$ is the adjoint of $\pi\lambda(a)$ in the sense that $(\pi\lambda(a)b, c)\lambda = (b, \pi\lambda(a^*)c)\lambda$ for all $b, c \in \mathbf{A}$. Guided by the theory of $*$-representations we now make the following definition ([3] p. 99).

DEFINITION 1.

A state λ of $\mathbf{A}$ is called *continuous* if the $\pi\lambda(a)$ extend to bounded operators on $\mathscr{H}_\lambda$ for each $a \in \mathbf{A}$.

Obviously, if λ is continuous, the $\pi\lambda(a)$ for self-adjoint a ($a^* = a$) form a set of commuting self-adjoint operators. This suggests making a second definition.

DEFINITION 2.

A state λ of $\mathbf{A}$ is called *regular* if for each self-adjoint $a, \pi\lambda$ is essentially self-adjoint on $\mathscr{H}_\lambda^0$, and the self-adjoint operators corresponding to different elements of $\mathbf{A}$ commute strongly.

Strong commutativity means the commutativity of the spectral projections or equivalently, the commutativity of the unitary groups generated by the self-adjoint extensions.

Let $\mathrm{Spec}(\mathbf{A})$ be the spectrum of $\mathbf{A}$, namely the set of homomorphisms of $\mathbf{A}$ into $\mathbf{C}$; it has an involution $h \to h^*$ given by $h^*(a) = h(a^*)^{\mathrm{conj}}$; the fixed points under this involution form the set $\mathrm{Spec}(\mathbf{A})_{\mathbf{R}}$ of $*$-homomorphisms of $\mathbf{A}$. We equip $\mathrm{Spec}(\mathbf{A})_{\mathbf{R}}$ (and $\mathrm{Spec}(\mathbf{A})$) with the smallest σ-algebra of sets with respect to which the evaluation maps $h \to h(a)$ ($a \in \mathbf{A}$) are all Borel. It is then natural to make the following definition.

DEFINITION 3.

A state λ of $\mathbf{A}$ is called *representable* if there exists a probability measure p on $\mathrm{Spec}(\mathbf{A})_{\mathbf{R}}$ such that

$$\lambda(a) = \int_{\mathrm{Spec}(\mathbf{A})_{\mathbf{R}}} a \, dp, \quad (a \in \mathbf{A}).$$

If p is unique (resp. has compact support), λ is called *uniquely representable* (resp. *compactly representable*).

The mutual relationships among these definitions are generally known and are summarized below. Let λ be a state of $\mathbf{A}$.

PROPOSITION 4.

(a) *If λ is regular, it is uniquely representable. If it is continuous it is regular.*
(b) *Suppose for each $a \in \mathbf{A}$ there is a number $t(a) > 0$ such that*

$$\Sigma_{n \geqslant 0} t(a)^n |\lambda(a^n)|/n! < \infty.$$

Then λ is regular.
(c) *λ is continuous $\Leftrightarrow \lambda$ is compactly representable $\Leftrightarrow$ for each $a \in \mathbf{A}$ there is a constant $L(a) \geqslant 1$ such that $|\lambda(a^n)| \leqslant L(a)^n$ for all $n \geqslant 0$.*
(d) *If $\mathbf{A}$ has a single self-adjoint generator, all of its states are representable.*

I do not prove this result since the proof involves only standard aspects of the spectral theory of self-adjoint operators. If $\mathbf{A}$ is the polynomial algebra the representability problem is just the classical problem of moments. It is classical that there is always a solution when the number of variables is 1 (this leads to (d)). I do not know whether the states of an arbitrary countably generated algebra are always

representable; if this is so, it would be of interest to examine the nature of the set of extreme points of the convex set of representing measures for a given state.

3. States and spectrum of $R(G)$

We have

Theorem 1. *Let G be a compact group and λ a state of $R(G)$. The following are equivalent:*
(a) *There are constants $C > 0, r \geqslant 0$ such that*

$$|\lambda(\tau)| \leqslant C \deg(\tau)^r$$

for all irreducible characters τ of G.
(b) *There is an invariant probability measure p on G such that*

$$\lambda(a) = \int_G a \, dp, \quad a \in R(G).$$

If these conditions are satisfied, p is unique and we have the estimate

$$|\lambda(\tau)| \leqslant \deg(\tau), \quad \tau \text{ irreducible.}$$

COROLLARY 2.

The state ν of Lemma 1.1 satisfies the above estimate and is hence represented by a unique invariant probability measure on G.

Proof. We begin with the Corollary. If $\tau \neq 1$ is an irreducible character,

$$\tau\tau^* = 1 + \Sigma_j m_j \tau_j.$$

where the m_j are integers > 0 and $\tau_j \neq 1$ are irreducible characters; and we have

$$0 \leqslant \nu(\tau\tau^*) = 1 - \Sigma_j m_j |\nu(\tau_j)| \leqslant 1.$$

Consequently,

$$|\nu(\tau)|^2 = |(\tau, 1)_\nu|^2 \leqslant (\tau, \tau)_\nu = \nu(\tau\tau^*) \leqslant 1$$

showing that the estimate in question is trivially true for ν.

We now take up the proof of the theorem. The non-trivial part is the implication (a)$\Rightarrow$(b). The uniqueness of p follows from the fact that $R(G)$ is dense in the Banach space of invariant continuous functions on G and $a \to \int_G a \, dp$ is a continuous linear functional.

It is enough to prove (a)$\Rightarrow$(b) when G is a Lie group. For, if this is done, we have unique invariant measures pH on the Lie quotients H of G representing the restriction of λ to $R(H) \subset R(G)$; and the uniqueness of pH shows that the system $\{(H, pH)\}$ is coherent, leading in a standard fashion to the required pG as $\lim_H pH$.

For a Lie group G let $\mathfrak{g} = \mathrm{Lie}(G)$ and let $X_1, \ldots, X_n$ be a basis for $\mathfrak{g}$, orthonormal with respect to the form $(X, Y) \to \mathrm{tr}(\mathrm{ad}\, X\, \mathrm{ad}\, Y)$ $(X, Y \in \mathfrak{g})$. Let the element $\square$ of the enveloping algebra of $\mathfrak{g}$ be given by

$$\square = 1 - (X_1^2 + \cdots + X_n^2).$$

Then $\square$ is independent of the choice of the basis and is invariant under the action of G. We shall now view $\square$ in the usual manner as a differential operator on G. If π is an irreducible representation of G, $\pi(\square)$ is a scalar depending only on the character τ of π, say $c(\tau)$. Clearly $c(\tau) \geqslant 1$. We then have the following ([5], pp. 316–318; (ii) may also be proved by Sobolev estimates for elliptic operators on compact manifolds). (i) There are constants $C > 0, r, s \geqslant 0$ such that

$$\deg(\tau) \leqslant C c(\tau)^r, \Sigma_\tau c(\tau)^{-s} < \infty,$$

where τ varies over the set of irreducible characters of G.
(ii) The collection of seminorms

$$C^\infty(G) \ni f \to \| \square^r f \|_2 = \left(\int_G |\square^r f|^2 \, \mathrm{d}x \right)^{1/2}$$

for $r = 0, 1, 2, \ldots$, already induces the topology of $C^\infty(G)$.

It follows from this that for f in $C^\infty(G)$,

$$\Sigma_\tau f\hat{}(\tau)\tau = f^\# := \int_G \mathrm{Ad}(u) f \, \mathrm{d}u,$$

the series converging absolutely in $C^\infty(G)$.

The key to the proof is to show that the estimates for λ permit us to extend λ uniquely to $C^\infty(G)$ as a *distribution* in the sense of L. Schwartz on G. Indeed, the estimates (a) shows that for some $m \geqslant 0$, $\lambda(\tau) = O(c(\tau)^m)$. Since $f\hat{}(\tau) = O(c(\tau)^{-q})$ for any $q \geqslant 0$, for any $f \in C^\infty(G)$, we can define

$$T(f) = \Sigma_\tau \lambda(\tau) f\hat{}(\tau) \quad (f \in C^\infty(G)).$$

Obviously $T = \lambda$ on $R(G)$.

It follows from the estimate

$$|f\hat{}(\tau)| \leqslant c(\tau)^{-q} \| \square^q f \|_2$$

that

$$|T(f)| \leqslant C \| \square^m f \|_2$$

showing that T is an invariant distribution on G. Since T is an extension of the state λ, it is clear that $T(ff^*) \geqslant 0$ for all invariant $f \in C^\infty(G)$, hence $T(g) \geqslant 0$ for all non-negative $g \in C^\infty(G)$, as T is invariant. But then T is a measure, by a classical result.

Example 1. Let $G = \mathrm{SU}(2)$, $G_{\mathbf{C}} = \mathrm{SL}(2, \mathbf{C})$ and let T (resp. $T_{\mathbf{C}}$) be the diagonal subgroup of G (resp. $G_{\mathbf{C}}$). The irreducible characters τ of G satisfy $\tau = \tau^*$ and so a homomorphism $\lambda(R(G) \to \mathbf{C})$ is a state as soon as $\lambda(\tau)$ is real for all τ. The irreducible characters of G

are the τ_n ($n \geqslant 0$) where

$$\tau_n(\mathrm{diag}(z, z^{-1})) = z^n + z^{n-2} + \cdots + z^{-n}.$$

Note that the elements of $R(G)$ are (holomorphic) functions on $G_{\mathbf{C}}$ and so evaluations at points of $G_{\mathbf{C}}$ define homomorphisms of $R(G)$. Since $\deg(\tau_n) = n + 1$, the estimate in Theorem 1 becomes $\lambda(\tau_n) = O(n^k)$ for some $k \geqslant 0$. Let r be a real number > 1 and let $g(r) = \mathrm{diag}(r, r^{-1})$. Then $\lambda(r)(\xi \to \xi(g(r)))$ is a state; but

$$|\lambda(r)(\tau_n)| = r^n + \cdots + r^{-n} \geqslant r^n + r^{-n}$$

and so $\lambda(r)$ cannot be represented by an invariant measure on G.

The point of this example is that $\mathrm{Spec}\, R(G)_{\mathbf{R}}$ is *not* exhausted by the conjugacy classes of G. Indeed, if we identify $R(G)$ with $\mathbf{C}[z, z^{-1}]^W$ where W is the reflexion $z \to z^{-1}$, we see that $\mathrm{Spec}(R(G)) = W\backslash\mathbf{C}$ and so $\mathrm{Spec}(R(G))$ gets identified with the set $\{r | r > 1\} \amalg (W\backslash\mathbf{T})$ ($\mathbf{T}$ = unit circle); only the points of $\mathbf{T}$ correspond to conjugacy classes in G.

The well-known representation theory of semi-simple groups can be used to show that essentially all aspects of this example generalize to the case where G is compact, semi-simple and simply connected. We may then view G as a real form of the complex group $C_{\mathbf{C}}$ whose Lie algebra $\mathfrak{g}_{\mathbf{C}}$ is the complexification of $\mathfrak{g} = \mathrm{Lie}(G)$. Let T be a maximal (topological) torus of G and $T_{\mathbf{C}}$ the maximal (algebraic) torus of $G_{\mathbf{C}}$ containing T. The compact group G defines the conjugation $\xi \to \xi^*$ in $R(G)$. Let

$$T_{\mathbf{R}} = \{t \in T_{\mathbf{C}} | \xi^*(t) = \xi(t)^* \text{ for all } \xi \in R(G)\}.$$

If W is the Weyl group of $(G_{\mathbf{C}}, T_{\mathbf{C}})$, it is obvious that $T, T_{\mathbf{C}}$ and $T_{\mathbf{R}}$ are all invariant under W. We have $T \subset T_{\mathbf{R}}$, but in general, $T \neq T_{\mathbf{R}}$. We select a positive chamber in $T_{\mathbf{C}}$ and parametrize the irreducible characters of G by τ_μ, μ a highest weight. We write $o(\mu)$ for the order of μ. The following theorem is then not difficult to establish.

Theorem 3. *A state of λ of $R(G)$ is continuous if and only if for some constant $D \geqslant 1$,*

$$|\lambda(\tau_\mu)| \leqslant D^{o(\mu)}$$

for all highest weights μ. The continuous states are precisely those uniquely represented as integrals with respect to compactly supported W-invariant probability measures over $T_{\mathbf{R}}$.

From the point of view of conjugacy classes, we know that $W\backslash T_{\mathbf{C}}$ is the space of all semi-simple conjugacy classes of $G_{\mathbf{C}}$. In the previous theorem we may actually assume that G is any compact Lie group, connected or not. Then $G_{\mathbf{C}}$ is defined as the spectrum of the algebra which is the (Hopf) algebra $H(G)$ of matrix coefficients of G. If we drop the assumption that G is Lie, $H(G)$ and $G_{\mathbf{C}}$ can still be defined and $G_{\mathbf{C}}$ becomes a proalgebraic group. It will be interesting to describe $\mathrm{Spec}(R(G))$ and $\mathrm{Spec}(R(G))_{\mathbf{R}}$ in terms of semi-simple conjugacy classes in this situation.

References

[1] Davenport H, *Multiplicative number theory* (Berlin: Springer Verlag) (1980)

[2] Deligne P, La conjecture de Weil. II, *Publ. Math. i. H.E.S.* **52** (1980) 138–252

[3] Loomis L, *Abstract harmonic analysis* (New York: Van Nostrand) (1953)
[4] Moreno C, The method of Hadamard and De la Vallée Poussin, *L'Enseignement Mathematique*, **29** (1983) 89–128
[5] Varadarajan V S, *Harmonic analysis on real reductive groups, Springer Lecture Notes in Mathematics*, **576** (1977)

Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 313–324.
© Printed in India.

On an approximate identity of Ramanujan

D ZAGIER
Max-Planck Institut für Mathematik, Gottfried-Claren-Straße 26, D-5300 Bonn, FRG and Department of Mathematics, University of Maryland, College Park, Maryland 20742, USA

Abstract. In his second notebook, Ramanujan says that

$$\frac{q}{x+}\frac{q^4}{x+}\frac{q^8}{x+}\frac{q^{12}}{x+}\cdots = 1-\frac{qx}{1+}\frac{q^2}{1-}\frac{q^3x}{1+}\frac{q^4}{1-}\cdots$$

"nearly" for q and x between 0 and 1. It is shown in what senses this is true. In particular, as $q \to 1$ the difference between the left and right sides is approximately $\exp\{-c(x)/(1-q)\}$ where $c(x)$ is a function expressible in terms of the dilogarithm and which is monotone decreasing with $c(0) = \pi^2/4, c(1) = \pi^2/5$; thus the difference in question is less than $2 \cdot 10^{-85}$ for $q = 0{\cdot}99$ and all x between 0 and 1.

Keywords. Approximate identity; asymptotic behaviour; Rogers–Ramanujan identities; dilogarithm function.

1. Introduction

Ramanujan's notebooks abound with assertions of strange identities, a good many of which have remained mysterious until now. I recently learned of one of these from Henri Cohen, to whom it had been shown by Bruce Berndt: on page 289, formula (4) of the Second Notebook, Ramanujan says that

$$1-\cfrac{qx}{1+\cfrac{q^2}{1-\cfrac{q^3x}{1+\cfrac{q^4}{1-\cfrac{q^5x}{1+\ddots}}}}} = \cfrac{q}{x+\cfrac{q^4}{x+\cfrac{q^8}{x+\cfrac{q^{12}}{x+\ddots}}}} \quad \text{"nearly"} \quad (1)$$

for q and x between 0 and 1. At first sight it is not even clear what this means; certainly the two continued fractions do not have the same power series expansions in q or x. However, Cohen did some computations and found that the two sides of (1) are numerically very close if q is near one, as shown in figure 1 or in the following small table giving the two values in question for $x = 0{\cdot}5$ or 1 and $q = 0{\cdot}8$, 0·9 and 0·95:

	$q = 0{\cdot}8$	$q = 0{\cdot}9$	$q = 0{\cdot}95$
$x = 0{\cdot}5$	0·774652...	0·7767340180...	0·77859859961698872648...
	0·774627...	0·7767340194...	0·77859859961698872686...
$x = 1$	0·59124...	0·605146977...	0·611726198935852157...
	0·59086...	0·605146958...	0·611726198935852104...

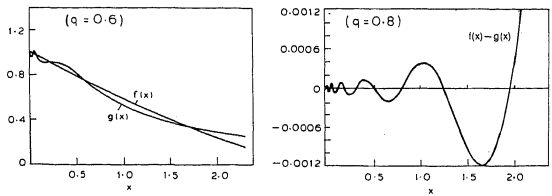


Figure 1. The functions $f(x)$ and $g(x)$ for $q = 0{\cdot}6$, $q = 0{\cdot}8$.

Cohen also showed that the two sides of (1) agree for $x = q$. Moreover, they both satisfy the same functional equation

$$(h(x) + qx)h(q^2x) = 1 \quad (q \text{ fixed}), \tag{2}$$

so that they in fact agree whenever x is equal to an odd power of q (we will give the proofs of these statements below). However, it remained to find a quantitative measure for the difference of the two expressions, in order to explain the extreme degree of nearness seen in the table. This is provided by the following result, whose proof is the object of the present paper.

Theorem. *For $0 < q < 1$ and $x > 0$ denote by $f(x) = f(x; q)$ and $g(x) = g(x; q)$ the left and right sides of (1), respectively. Then:*

(I) *For $x = 1$, we have $f(1) - g(1) = O(\exp\{(\pi^2/5)/\log q\})$. More precisely, setting $Q = \exp\{(\pi^2/5)/\log q\}$ we have*

$$f(1) = q^{\frac{1}{2}}\frac{\sqrt{5}-1}{2}\left(1 + \sqrt{5}Q + \frac{5-\sqrt{5}}{2}Q^2 - \frac{5-3\sqrt{5}}{2}Q^3 - \cdots\right),$$

$$g(1) = q^{\frac{1}{2}}\frac{\sqrt{5}-1}{2}\left(1 - \sqrt{5}Q + \frac{5-\sqrt{5}}{2}Q^2 + \frac{5-3\sqrt{5}}{2}Q^3 - \cdots\right)$$

and in particular $f(1) - g(1) = (5 - \sqrt{5})q^{\frac{1}{2}}Q + O(Q^2)$ as $q \to 1$.

(II) *For $x \to 0$ we have $f(x) - g(x) = O(\exp\{(\pi^2/4)/\log q\})$. More precisely, setting $Q = \exp\{(\pi^2/4)/\log q\}$ and $\theta = (\pi \log x)/(2 \log q)$ we have*

$$f(x) = 1 + O(x),$$

$$g(x) = \frac{1 - 2Q\cos\theta + 2Q^4\cos 2\theta - 2Q^9\cos 3\theta + \cdots}{1 + 2Q\cos\theta + 2Q^4\cos 2\theta + 2Q^9\cos 3\theta + \cdots} + O(x),$$

and in particular $f(x) - g(x) = 4Q\cos(\pi\lambda/2) + O(Q^2)$ as $x \to 0$ through a sequence $x = q^{4n+\lambda}$, $n \to \infty$.

(III) *In general $f(x) - g(x) = \exp\{[c(x) + o(1)]/\log q\}\cos\theta$ for $q \to 1$ with θ as in* (II)

and

$$c(x) = \frac{\pi^2}{6} + \tfrac{1}{2}Li_2(((1+x^2/4)^{\frac{1}{2}} - x/2)^2)$$

$$+ \tfrac{1}{2}\log^2((1+x^2/4)^{\frac{1}{2}} + x/2) - \log(x)\log((1+x^2/4)^{\frac{1}{2}} + x/2)$$

$$\left(Li_2(t) = \sum_{n=1}^{\infty} \frac{t^n}{n^2} \textit{ the dilogarithm function}\right).$$

The theorem implies, for instance, that for $q = 0{\cdot}99$ the left- and right-hand sides of (1) agree to about 85 decimal digits for x near 1, to about 96 digits for x near $\frac{1}{2}$, ($c(\frac{1}{2}) = 2.218\ldots$), and to about 107 digits for x near 0.

The known values $Li_2(1) = \pi^2/6$ and $Li_2(\frac{1}{2}(3-\sqrt{5})) = (\pi^2/15) - \log^2(\frac{1}{2}(1+\sqrt{5}))$ ([2], 1.4.1) imply $c(0) = \pi^2/4, c(1) = \pi^2/5$, so the formula of part (III) is compatible with the assertions in (I) and (II). A graph of the function $c(x)$ is shown in figure 2. Notice that $c(x)$ becomes negative for x larger than about 6.177, so for x this large the difference between the two sides of (1) becomes exponentially big rather than exponentially small as $q \to 1$.

In the next section of the paper we give some simple transformations of the continued fractions in (1). Sections 3 to 5 contain the proofs of assertions (I), (II), and (III), respectively, and we conclude with some speculations about what Ramanujan himself had in mind when stating (1).

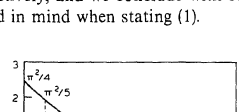


Figure 2. Graph of $c(x)$.

2. Preliminaries

In this section we give various representations of $f(x)$ and $g(x)$ as quotients of infinite sums. The formulae in the first proposition were given by Berndt.

PROPOSITION 1.

Define power series $F(x) = F(x;q) \in \mathbb{Z}[[q,x]]$ *and* $G(x) = G(x;q) \in \mathbb{Z}[[q,x^{-1}]]$ *by*

$$F(x) = \sum_{n=0}^{\infty} \frac{q^{n^2+n}}{(1-q^2)(1-q^4)\cdots(1-q^{2n})(1-q^3x)(1-q^5x)\cdots(1-q^{2n+1}x)},$$

$$G(x) = \sum_{n=0}^{\infty} \frac{x^{-2n}q^{4n^2}}{(1-q^4)(1-q^8)\cdots(1-q^{4n})}.$$

Then

$$f(x) = (1 - qx)\frac{F(q^{-2}x)}{F(x)}, \quad g(x) = \frac{q}{x}\frac{G(q^{-2}x)}{G(x)}.$$

The functions $F(x)$ and $G(x)$ satisfy the recursions

$$\frac{1}{1 - qx}F(x) = q^{-1}xF(q^{-2}x) + (1 - q^{-1}x)F(q^{-4}x),$$

$$G(x) = G(q^{-2}x) + q^4x^{-2}G(q^{-4}x).$$

An immediate corollary is that both $h = f$ and $h = g$ satisfy the recursion (2).

Proof.

(i) For $j \geqslant 0$ define $F_j(x)$ like $F(x)$ but with q^{n^2+n} replaced by $q^{n^2+(2j+1)n}$ in the numerator. Then for $j \geqslant 1$

$$F_{j-1}(x) - F_j(x) = \sum_{n=1}^{\infty} \frac{q^{n^2+(2j-1)n}}{(1 - q^2)\cdots(1 - q^{2n-2})(1 - q^3x)\cdots(1 - q^{2n+1}x)}$$

$$= \frac{q^{2j}}{1 - q^3x}F_j(q^2x)$$

and

$$F_{j-1}(q^{-2}x) - F_{j-1}(x)$$

$$= qx\sum_{n=1}^{\infty} \frac{q^{n^2+(2j-1)n}}{(1 - q^2)\cdots(1 - q^{2n-2})(1 - qx)(1 - q^3x)\cdots(1 - q^{2n+1}x)}$$

$$= \frac{q^{2j+1}x}{(1 - qx)(1 - q^3x)}F_j(q^2x).$$

These two equations give for $j = 1$ the recurrence for $F_0 = F$ stated in the Proposition, and for $j \geqslant 1$ the recurrence

$$f_{j-1}(x) = 1 - q^{2j-1}x/(1 + q^{2j}/f_j(x))$$

for the quantities $f_j(x) = (1 - q^{2j+1}x)F_j(q^{2j-2}x)/F_j(q^{2j}x)$. It now follows by induction that $f_0 = f$ as claimed.

(ii) We have

$$G(x) - G(q^{-2}x) = \sum_{n=1}^{\infty} \frac{x^{-2n}q^{4n^2}}{(1 - q^4)\cdots(1 - q^{4n-4})}$$

$$= \sum_{n=0}^{\infty} \frac{x^{-2(n+1)}q^{4(n+1)^2}}{(1 - q^4)\cdots(1 - q^{4n})} = q^4x^{-2}G(q^{-4}x).$$

Replacing x by $q^{-2n+2}x$ and rearranging, we find

$$xG(q^{-2n+2}x)/G(q^{-2n}x) = x + \frac{q^{4n}}{xG(q^{-2n}x)/G(q^{-2n-2}x)} \quad (n \geqslant 1)$$

and hence by induction $xG(x)/G(q^{-2}x) = q/g(x)$ as asserted. □

The representation for f is a little more awkward than that for g because $F(x)$ has poles at $x = q^{-3}, q^{-5}, \ldots$. To eliminate these, set

$$\hat{F}(x) = (1 - q^3x)(1 - q^5x)\cdots F(x).$$

Then both the recursion for F and the formula for f become simpler:

$$\hat{F}(x) = q^{-1}x\hat{F}(q^{-2}x) + \hat{F}(q^{-4}x), \quad f(x) = \frac{\hat{F}(q^{-2}x)}{\hat{F}(x)}. \tag{3}$$

Write $\hat{F}(x) = \sum_{n=0}^{\infty} a_n x^n$ where $a_n \in \mathbb{Z}[[q]]$. Comparing coefficients of x^n in the first equation in (3) gives $(1 - q^{-4n})a_n = q^{-2n+1}a_{n-1}$, so by induction

$$a_n = \frac{(-1)^n q^{n^2+2n}}{(1-q^4)(1-q^8)\cdots(1-q^{4n})} a_0.$$

Now writing $H(x)$ for $a_0^{-1}\hat{F}(q^{-2}x)$ (the value of a_0 is irrelevant; it is in fact equal to $\prod_1^{\infty}(1+q^{2n})$) we have

PROPOSITION 2.

Define $H(x) = H(x; q) \in \mathbb{Z}[[q, x]]$ *by*

$$H(x) = \sum_{n=0}^{\infty} \frac{(-1)^n q^{n^2} x^n}{(1-q^4)(1-q^8)\cdots(1-q^{4n})}.$$

Then $H(x) = -qxH(q^2x) + H(q^4x)$ *and* $f(x) = H(x)/H(q^2x)$. □

Of course, we could have proved this directly by an argument similar to the proof of Proposition 1 and avoided introducing F entirely.

3. Asymptotic behaviour for $x = 1$; the Rogers–Ramanujan identities

Define a function $\zeta(z)$ in the upper half-plane $\mathfrak{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by

$$\zeta(z) = \cfrac{q^{\frac{1}{5}}}{1 + \cfrac{q}{1 + \cfrac{q^2}{1 + \ddots}}} \quad (z \in \mathfrak{H}), \tag{4}$$

where $q = \exp(2\pi i z)$ and q^λ for $\lambda \in \mathbb{Q}$ denotes $\exp(2\pi i \lambda z)$. For $x = 1$, both continued fractions in (1) can be expressed in terms of ζ:

$$f(1;q) = -q^{\frac{1}{5}}/\zeta(z+\tfrac{5}{2}), \quad g(1;q) = q^{\frac{1}{5}}\zeta(4z) \quad (q = \exp(2\pi i z), z \in \mathfrak{H}). \tag{5}$$

The key to understanding the behaviour of $f(1)$ and $g(1)$ as $q \to 1$ is the fact that $\zeta(z)$ is a modular function, namely

$$\zeta(\gamma\langle z\rangle) = \zeta(z) \quad \forall \gamma \in \Gamma(5), \quad z \in \mathfrak{H},$$

where

$$\Gamma(5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Z}, ad-bc = 1, a \equiv d \equiv 1 \pmod 5, b \equiv c \equiv 0 \pmod 5 \right\}$$

and $\gamma\langle z\rangle$ for a 2×2 matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of determinant 1 denotes the image $(az+b)/(cz+d)$ of z under the associated fractional linear transformation. This fact, well known to Ramanujan, follows from the Roger–Ramanujan identities. Recall that these are the formulae

$$\sum_{n=0}^{\infty} \frac{q^{n^2}}{(1-q)\cdots(1-q^n)} = \prod_{n \equiv \pm 1 (5)} (1-q^n)^{-1},$$

$$\sum_{n=0}^{\infty} \frac{q^{n^2+n}}{(1-q)\cdots(1-q^n)} = \prod_{n \equiv \pm 2 (5)} (1-q^n)^{-1}$$

([1], Theorem 362 and 363). The left-hand sides of these equations are $G(1;q^{\frac{1}{5}})$ and $G(q^{-\frac{1}{5}};q^{\frac{1}{5}})$, respectively, where $G(x;q)$ is defined as in Proposition 1, so by (5) and that Proposition we have

$$\zeta(z) = q^{-\frac{1}{60}} g(1;q^{\frac{1}{5}}) = \frac{q^{\frac{1}{5}} G(q^{-\frac{1}{5}};q^{\frac{1}{5}})}{G(1;q^{\frac{1}{5}})} = q^{\frac{1}{5}} \prod_{n=1}^{\infty} (1-q^n)^{(n/5)}$$

($(n/5)$ = Legendre symbol $= +1, -1, 0$ for $n \equiv \pm 1, \pm 2, 0 \pmod 5$, respectively). On the other hand, we have

$$\prod_{n \equiv 0, \pm 1 (5)} (1-q^n) = \sum_n (-1)^n q^{\frac{1}{2}(5n^2+3n)}$$

$$\prod_{n \equiv 0, \pm 2 (5)} (1-q^n) = \sum_n (-1)^n q^{\frac{1}{2}(5n^2+n)}$$

by the Jacobi triple product identity ([1], Theorems 355 and 356), so this can be written

$$\zeta(z) = \frac{\theta_{10,3}(z)}{\theta_{10,1}(z)}, \quad \theta_{10,j}(z) = \sum_n (-1)^n q^{(10n+j)^2/40} \quad (j = 1, 3). \tag{6}$$

This equation makes it clear that $\zeta(z)$ is a modular function, since both theta-series $\theta_{10,3}(z)$ and $\theta_{10,1}(z)$ are modular forms of weight $\frac{1}{2}$. In fact $\zeta(z)$ is a well-known modular function called Klein's icosahedral function. It is a "Hauptmodul" for $\Gamma(5)$, i.e., defines an isomorphism from $\mathfrak{H}/\Gamma(5) \cup \{\text{cusps}\}$ to $\mathbb{P}^1(\mathbb{C})$.

We will not give the proof of the invariance of $\zeta(z)$ under $\Gamma(5)$, since in view of (5)

what we actually need are the transformation laws satisfied by $\zeta(z)$ with respect to matrices sending the cusps 0 and $\frac{5}{2}$ to infinity. To obtain these, recall that the Poisson summation formula implies

$$\sum_{n=1}^{\infty} \chi(n)e^{-\pi n^2 t/f} = \frac{G(\chi)}{(ft)^{\frac{1}{2}}} \sum_{n=1}^{\infty} \bar{\chi}(n)e^{-\pi n^2/ft} \quad (\Re(t) > 0) \tag{7}$$

for any even primitive Dirichlet character χ of conductor $f > 1$, where $G(\chi)$ is the Gauss sum $\sum_{n=1}^{f} \chi(n)\cos(2\pi n/f)$ associated to χ, a complex number of absolute value $\sqrt{f}$. Applying this to the two primitive even characters of conductor 20 gives

$$\theta_{10,1}(it) \pm i\theta_{10,3}(it) = \frac{2\sin(2\pi/5)}{(5t)^{\frac{1}{2}}}\left(1 \pm i\frac{\sqrt{5}-1}{2}\right)\left(\theta_{10,1}\left(\frac{i}{t}\right) \mp i\theta_{10,3}\left(\frac{i}{t}\right)\right)$$

and hence from (6)

$$\zeta(it) = \frac{\dfrac{\sqrt{5}-1}{2} - \zeta\left(\dfrac{i}{t}\right)}{1 + \dfrac{\sqrt{5}-1}{2}\zeta\left(\dfrac{i}{t}\right)}.$$

Inserting this into the second of equation (5) and letting t tend to 0 through positive real values, we find

$$g(1;q) = q^{\frac{1}{5}} \frac{\dfrac{\sqrt{5}-1}{2} - \zeta\left(\dfrac{-\pi i}{2\log q}\right)}{1 + \dfrac{\sqrt{5}-1}{2}\zeta\left(\dfrac{-\pi i}{2\log q}\right)}$$

$$= q^{\frac{1}{5}} \frac{\sqrt{5}-1}{2} \frac{1 - \frac{1}{2}(\sqrt{5}+1)Q/(1+Q^5/(1+Q^{10}/(1+\cdots)))}{1 + \frac{1}{2}(\sqrt{5}-1)Q/(1+Q^5/(1+Q^{10}/(1+\cdots)))}$$

($Q = \exp\{(\pi^2/5)/\log q\}$), giving the second formula in (I) of the Theorem. Similarly (7) applied to the two non-real even primitive characters of conductor 40 gives

$$\theta_{10,1}(\tfrac{1}{2}(5+it)) \pm i\theta_{10,3}(\tfrac{1}{2}(5+it))$$

$$= \frac{2\sin(\pi/5)}{\sqrt{5}}(1 \mp \tfrac{1}{2}(\sqrt{5}+1)i)(\theta_{10,1}(\tfrac{1}{2}(5+i/t)) \mp i\theta_{10,3}(\tfrac{1}{2}(5+i/t)))$$

and hence by (6) and (5)

$$\zeta\left(\frac{5+it}{2}\right) = \frac{\frac{1}{2}(\sqrt{5}+1) - \zeta(\frac{1}{2}(5+i/t))}{-1 + \frac{1}{2}(\sqrt{5}+1)\zeta(\frac{1}{2}(5+i/t))},$$

$$f(1;q) = q^{\frac{1}{5}} \frac{\sqrt{5}-1}{2} \frac{1 + \frac{1}{2}(\sqrt{5}+1)Q/(1-Q^5/(1-Q^{10}/(1-\cdots)))}{1 - \frac{1}{2}(\sqrt{5}-1)Q/(1-Q^5/(1-Q^{10}/(1-\cdots)))},$$

giving the first formula in (I) also.

Write the function $H(x)$ of Proposition 2 as $H_+(x) + H_-(x)$, where

$$H_\pm(x) = \pm \sum_{\substack{n \geqslant 0 \\ (-1)^n = \pm 1}} \frac{q^{n^2} x^n}{(1-q^4)\cdots(1-q^{4n})},$$

so that $H_+(x) \in \mathbb{Z}[x^2][[q^4]]$, $H_-(x) \in qx\mathbb{Z}[x^2][[q^4]]$. As a refinement of the recursion $H(x) = -qxH(q^2x) + H(q^4x)$ of Proposition 2 we have

$$\begin{aligned} H_\pm(x) - H_\pm(q^4x) &= \pm \sum_{\substack{n \geqslant 1 \\ (-1)^n = \pm 1}} \frac{q^{n^2} x^n}{(1-q^4)\cdots(1-q^{4n-4})} \\ &= \pm \sum_{\substack{n \geqslant 0 \\ (-1)^n = \mp 1}} \frac{q^{(n+1)^2} x^{n+1}}{(1-q^4)\cdots(1-q^{4n})} = -qxH_\mp(q^2x). \end{aligned}$$

An equivalent formulation of this is that the 2×2 matrix

$$\mathscr{H}(x) = \begin{pmatrix} H_+(x) & H_-(x) \\ H_-(q^2x) & H_+(q^2x) \end{pmatrix}$$

satisfies the recursion

$$\mathscr{H}(q^2x) = \begin{pmatrix} 0 & 1 \\ 1 & qx \end{pmatrix} \mathscr{H}(x) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{8}$$

This implies that the determinant of $\mathscr{H}(x)$ is invariant under $x \mapsto q^2x$ and hence, since $\mathscr{H}(x)$ tends to the identity matrix for $x \to 0$ with q fixed, that $\det \mathscr{H}(x) = 1$ identically. Now the content of Proposition 2 can be reformulated as

$$f(x) = \mathscr{H}(x)\langle 1 \rangle, \tag{9}$$

where $\langle\ \rangle$ denotes fractional linear transformation as in § 3. The key to Ramanujan's assertion is that $g(x)$, the second expression in (1), is given by

$$g(x) = \mathscr{H}(x)\langle \lambda(x) \rangle \tag{10}$$

where

$$\lambda(x) = \lambda(x; q) = \frac{\theta_-(x)}{\theta_+(x)}, \quad \theta_\pm(x) = \sum_{\substack{n \in \mathbb{Z} \\ (-1)^n = \pm 1}} q^{n^2} x^n. \tag{11}$$

Indeed, by applying the Poisson summation formula to θ_+ and θ_- as in the last section (this is of course the most classical application of the Poisson summation formula, going back to Jacobi), we obtain

$$\lambda(x) = \frac{1 - 2Q\cos\theta + 2Q^4\cos 2\theta - 2Q^9\cos 3\theta + \cdots}{1 + 2Q\cos\theta + 2Q^4\cos 2\theta + 2Q^9\cos 3\theta + \cdots} \tag{12}$$

where $Q = \exp((\pi^2/4)/\log q)$, $\theta = (\pi/2)(\log x/\log q)$, and since $\mathscr{H}(x) = \mathbf{1}_2 + O(x)$ we immediately deduce from (10) the assertion of part (II) of the Theorem.

Equation (10) follows immediately from Proposition 1 and

PROPOSITION 3.

Denote by $\vec{G}(x)$ *and* $\vec{\theta}(x)$ *the vectors*

$$\begin{pmatrix} qx^{-1}G(q^{-2}x) \\ G(x) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \theta_-(x) \\ \theta_+(x) \end{pmatrix},$$

respectively. Then $\vec{G}(x) = c \cdot \mathscr{H}(x)\vec{\theta}(x)$ *where* c *is a scalar independent of* x.

(In fact $c = \prod_{n=1}^{\infty}(1-q^{4n})^{-1}$, but we do not need this fact and will omit the proof.)

Proof. The recursion satisfied by $G(x)$ can be written in terms of $\vec{G}(x)$ as

$$\vec{G}(q^2x) = q^{-1}x^{-1}\begin{pmatrix} 0 & 1 \\ 1 & qx \end{pmatrix}\vec{G}(x).$$

Combining this with (8) we see that the vector $\vec{t}(x) = \mathscr{H}(x)^{-1}\vec{G}(x)$ satisfies the recursion

$$\vec{t}(q^2x) = q^{-1}x^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\vec{t}(x). \tag{13}$$

Write $\vec{t}(x)$ as $\begin{pmatrix} t_-(x) \\ t_+(x) \end{pmatrix}$. Since $G(x)$ is an even power series in x we have

$$\vec{G}(x) = \begin{pmatrix} \text{odd} \\ \text{even} \end{pmatrix}, \quad \mathscr{H}(x) = \begin{pmatrix} \text{even} & \text{odd} \\ \text{odd} & \text{even} \end{pmatrix}$$

(where "odd" and "even" denote even and odd functions of x), so $t_-(x)$ is odd and $t_+(x)$ is even, i.e.,

$$t_{\pm}(x) = \sum_{(-1)^n = \pm 1} t_n x^n$$

for some coefficients $t_n \in \mathbb{Z}[[q]]$. (Note that all coefficients of $\mathscr{H}$, $\vec{G}$, $\vec{\theta}$ and $\vec{t}$ are in the ring $\mathbb{Z}[x, x^{-1}][[q]]$ and can be expanded as doubly infinite Laurent series in x with coefficients in $\mathbb{Z}[[q]]$.) The recursion (13) now gives $t_{n+1} = q^{2n+1}t_n$ for all $n \in \mathbb{Z}$, so $t_n = t_0 q^{n^2}$. This proves Proposition 3 with $c = t_0$. □

The fact that the recursion (13) is satisfied by $\vec{\theta} = c^{-1}\vec{t}$ as well as by $\vec{t}$ says that $\theta_{\pm}(q^2x) = q^{-1}x^{-1}\theta_{\mp}(x)$. Therefore $\lambda(x)$ is changed to its reciprocal under $x \mapsto q^2x$ and hence is invariant under $x \mapsto q^4x$, which is why $\lambda(x)$ must have a Fourier series expansion in $\theta = (\pi/2)(\log x/\log q)$ (as given explicitly in (12)). The property $\lambda(q^2x) = \lambda(x)^{-1}$ together with the obvious symmetry property $\lambda(x^{-1}) = \lambda(x)$ implies that $\lambda(x) = 1$

$$\sum_{n\,\text{odd}} q^{n^2+n} = \sum_{n\,\text{even}} q^{n^2+n}$$

via $n \to -1-n$), so (9) and (10) imply Cohen's result that $f(x)$ and $g(x)$ agree for such x. Finally, instead of using just $\mathscr{H}(x) = \mathbf{1}_2 + O(x)$ we could use the full expansion

$$\mathscr{H}(x) = \begin{pmatrix} 1 + \dfrac{q^4x^2}{(1-q^4)(1-q^8)} + \cdots & -\dfrac{qx}{1-q^4} - \cdots \\ -\dfrac{q^3x}{1-q^4} - \cdots & 1 + \dfrac{q^8x^2}{(1-q^4)(1-q^8)} + \cdots \end{pmatrix}$$

and thus replace the formula in (II) of the Theorem by a full expansion in powers of x for $\theta \pmod{2\pi}$ fixed (i.e. for x tending to 0 through a sequence $q^{4n}x_0, n \to \infty$). In particular, to two terms we have

$$f(x) = 1 - \frac{q}{1+q^2}x + \mathrm{O}(x^2), \quad g(x) = \lambda(x) - \mu(x)x + \mathrm{O}(x^2) \quad \text{for} \quad x \to 0,$$

where $\mu(x)$ is the periodic function

$$\mu(x) = \frac{q}{1-q^4}(1 - q^2\lambda(x)^2) \quad \left(= \frac{q}{1+q^2} + \mathrm{O}(Q) \text{ as } q \to 1 \right).$$

5. Asymptotic behaviour for x arbitrary: the dilogarithm function

In the last two sections we studied the asymptotics of $f(x;q) - g(x;q)$ as $q \to 1$ for $x = 1$ and x near 0. We now study how these asymptotics change as x changes. Write $\varepsilon(x) = \varepsilon(x;q)$ for $f(x) - g(x)$. Subtracting the functional equation (2) with $h = g$ from the same equation with $h = f$, we find

$$\begin{aligned} 0 &= (g(x) + \varepsilon(x) + qx)(g(q^2x) + \varepsilon(q^2x)) - (g(x) + qx)g(q^2x) \\ &= \varepsilon(x)f(q^2x) + \varepsilon(q^2x)g(q^2x)^{-1} \end{aligned}$$

or

$$\varepsilon(x) = -\frac{1}{f(q^2x)g(q^2x)}\varepsilon(q^2x).$$

By induction this gives

$$\varepsilon(x) = \frac{(-1)^n}{f(q^2x)g(q^2x)\cdots f(q^{2n}x)g(q^{2n}x)}\varepsilon(q^{2n}x). \tag{14}$$

As $n \to \infty$ we have

$$q^{2n}x \to 0, \quad f(q^{2n}x) \to 1, \quad g(q^{2n}x) \to \begin{cases} \lambda(x) & \text{for } n \text{ even} \\ \lambda(q^2x) = \lambda(x)^{-1} & \text{for } n \text{ odd,} \end{cases}$$

by the results of the last section (specifically, by equations (9) and (10) and the periodicity $\lambda(q^4x) = \lambda(x)$), so letting $n \to \infty$ in (14) gives the closed formula

$$\varepsilon(x) = \left(\prod_{n=1}^{\infty} \frac{1}{f(q^{4n-2}x)g(q^{4n-2}x)f(q^{4n}x)g(q^{4n}x)} \right)(1 - \lambda(x)), \tag{15}$$

where the nth term of the product tends to 1 with exponential rapidity. We use equations (14) and (15) to study the asymptotics of $\varepsilon(x;q)$ as $q \to 1$ with x fixed. (Actually, this is not quite right since as $\log x/\log q$ varies modulo 4 the value of ε will oscillate; thus we should either let q tend to 1 continuously and restrict x to lie in an interval $[q^{-2}x_0, q^2x_0]$ with $\log x/\log q \pmod 4$ constant, or else fix x and let q tend to 1 through a sequence of values for which $\log x/\log q \pmod 4$ is constant.) In fact, since the behaviour of $1 - \lambda(x)$ as $q \to 1$ is completely known—it is asymptotically equal to $4\exp\{(\pi^2/4)/\log q\}\cos[(\pi/2)(\log x/\log q)]$— and since both $\varepsilon(x)$ and $1 - \lambda(x)$ vanish whenever x is an odd power of q, it is more convenient to study the ratio $\varepsilon(x)/(1 - \lambda(x))$, the first factor in (15). It is also natural to consider the $(\log q)$th power of this, i.e. to define a new quantity $A(x;q)$ by

$$\varepsilon(x;q) = (1 - \lambda(x;q))A(x;q)^{1/\log q}, \tag{16}$$

because by parts (I) and (II) of the Theorem we know that $A(x;q)$ has the well-defined limits $e^{-\pi^2/20}$ and 1 as $x \to 1$, $q \to 1$ and $x \to 0$, $q \to 1$, respectively. We want to show that $A(x;q)$ tends to a limit as $q \to 1$ for any x, and to evaluate this limit.

The first thing to notice is that $g(x;q)$ tends to a well-defined limit as $q \to 1$, since the continued fraction on the right of (1) converges at $q = 1$ for all $x > 0$. Call this limit $\gamma(x)$; then $\gamma(x) = 1/(x + \gamma(x))$ and consequently

$$\gamma(x) = (1 + x^2/4)^{\frac{1}{2}} - x/2.$$

The continued fraction on the left of (1) also converges for $q = 1$ if x is sufficiently small (actually, as one easily checks, for $x < 2$), and it must have the same limit $\gamma(x)$ because of the functional equation (2). On the other hand, equation (14) implies

$$A(q^{4n}x;q) = (f(q^2x)g(q^2x)f(q^4x)g(q^4x)\cdots f(q^{4n}x)g(q^{4n}x))^{\log q}A(x;q). \tag{17}$$

Choose a small number δ and let $q \to 1$ and $n \to \infty$ in such a way that $q^{4n} = e^{-\delta}$. Then each factor $f(q^{2i}x)$ and $g(q^{2i}x)$ in (17) equals $\gamma(x) + O(\delta)$ for $q \to 1$, so (17) gives

$$\begin{aligned} A(e^{-\delta}x;q) &= (\gamma(x) + O(\delta))^{4n\log q}A(x;q) = (\gamma(x) + O(\delta))^{-\delta}A(x;q) \\ &= (1 - \delta\gamma(x) + O(\delta^2))A(x;q) \quad (q \to 1). \end{aligned}$$

Together with the fact that $\lim_{x\to 0} A(x;q) = 1$ for all q, this shows that $A(x;q)$ for $q \to 1$ has a limit $A(x)$ which satisfies $A'(x) = (\gamma(x)/x)A(x)$ and $A(0) = 1$, or equivalently

$$A(x) = e^{c(x) - \pi^2/4}, \quad c(x) = \frac{\pi^2}{4} + \int_0^x \frac{1}{t}\log\left[\left(1 + \frac{t^2}{4}\right)^{\frac{1}{2}} - \frac{t}{2}\right]dt. \tag{18}$$

In view of (16) and the known asymptotics of $1 - \lambda(x)$ for $q \to 1$, this proves (III) of the Theorem except for the evaluation of the integral $c(x)$. Setting $t = 2y$ and integrating

by parts, we find

$$c(x) = \frac{\pi^2}{4} - \log\left(\frac{x}{2}\right)\log\left[\left(1+\frac{x^2}{4}\right)^{\frac{1}{2}} + \frac{x}{2}\right] + \int_0^{x/2} \frac{\log y}{(1+y^2)^{\frac{1}{2}}}\,dy.$$

The integral is evaluated in [2] (A.3.1.(6)) in terms of the dilogarithm, and this gives the formula asserted in the Theorem (up to the evaluation of the constant, which is fixed by $c(0) = \pi^2/4$, $Li_2(1) = \pi^2/6$). As mentioned in the introduction, the formula $c(1) = \pi^2/5$, which we know to be true by (II) of the Theorem, is equivalent to the special value $Li_2((3-\sqrt{5})/2) = \pi^2/15 - \log^2((1+\sqrt{5})/2)$ of the dilogarithm, a value well known to Ramanujan.

6. Final remarks

In this paper we have made Ramanujan's assertion (1) precise in various senses and given proofs of these statements. It is reasonable to ask how much of what we have done Ramanujan actually had in mind. Obviously this is pure speculation. I would guess that he knew (I) of the Theorem, since the function defined by the continued fraction (4) was a favourite of his, and that he knew the magic identity (10), which—since he certainly knew (9) and that $\lambda(x)$ is very close to 1—would suffice to imply (1) in the rough form stated. I do not think that he knew the full asymptotics of $f - g$ for $q \to 1$ as given in (III) of the Theorem, since he was particularly fond of the dilogarithm and of its evaluation at special arguments and would hardly have failed to at least mention the formula in his notebook. As to how he might have discovered (10), I have no idea, since I absolutely do not know where this identity comes from. I myself found it by the stupid method of evaluating the difference $f(x;q) - g(x;q)$ for hundreds of values of x and q and thus discovering numerically that $g(x)$ for x small had the Fourier expansion given in (II); this at least suggested looking at the theta-series $\theta_+(x)$ and $\theta_-(x)$, after which it was not too hard to discover the matrix $\mathscr{H}(x)$ and the identity (10) (the proofs, of course, were easy once the formulae were known, as in all identities of this type). Such extensive numerical computations would be impossible without a computer even for a Ramanujan—but then again a Ramanujan would not (and in this case did not) need them to discover mysterious and beautiful identities which would be hidden to ordinary mortals.

References

[1] Hardy G H and Wright E M, *An introduction to the theory of numbers, 4th ed.* (Oxford: University Press) (1960)

[2] Lewin L, *Polylogarithms and associated functions*, (New York: North Holland) (1981)

Note added in proof

While in India for the Ramanujan centenary celebrations, I learned that a formula equivalent to (10) *is* in fact contained in Ramanujan's "Lost Notebook".

Proceedings (Mathematical Sciences)

Volume 97, 1987

SUBJECT INDEX

Approximate identity
On an approximate identity of Ramanujan 313
Arithmetic Siegel modular functions
On the proof of the reciprocity law for arithmetic Siegel modular functions 21
Asymptotic behaviour
On an approximate identity of Ramanujan 313
Automorphic cuspidal representations
On Whittaker models and the vanishing of Fourier coefficients of cusp forms 67
Automorphic representation
On the nonvanishing of some L-functions 117

Basic hypergeometric series
On some generalizations of Ramanujan's continued fraction identities 31
Bounded covolume
On the set of discrete subgroups of bounded covolume in a semisimple group 45

Character ring
The states of the character ring of a compact group 305
Class numbers
Traces of Eichler–Brandt matrices and type numbers of quaternion orders 189
Commutative rings
On endomorphisms of degree two 179
Compact group
The states of the character ring of a compact group 305
Composition of quadratic forms
On endomorphisms of degree two 179
Conjugacy class of endomorphism
On endomorphisms of degree two 179
Continued fractions
Hypergeometric series and continued fractions 277
Cusp forms
On Whittaker models and the vanishing of Fourier coefficients of cusp forms 67
Cuspidal class group
The Manin–Drinfeld theorem and Ramanujan sums 251

Deligne's generalization
The states of the character ring of a compact group 305
Dilogarithm function
On an approximate identity of Ramanujan 313
Discrete subgroups
On the set of discrete subgroups of bounded covolume in a semisimple group 45

Eichler–Brandt matrices
Traces of Eichler–Brandt matrices and type numbers of quaternion orders 189
Eisenstein series
The Manin–Drinfeld theorem and Ramanujan sums 251
Elliptic curves
On the supersingular reduction of elliptic curves 247
Estimation of area
The area within a curve 111
Euler's phi function
Fluctuations in the mean of Euler's phi function 239
Exponential sums
On exponential sums involving the Ramanujan function 157
Approximation of exponential sums by shorter ones 167

Fluctuations
Fluctuations in the mean of Euler's phi function 239

(GL_n, GL_m)-duality
(GL_n, GL_m)-duality and symmetric plethysm 85

Hadamard–Vallee Poussin method
The states of the character ring of a compact group 305
Hardy–Ramanujan formula
Multiplicative properties of the partition function 297

Hecke-algebra
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201
Hurwitz order
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201

Hypergeometric series
Hypergeometric series and continued fractions 277
Almost poised basic hypergeometric series 61

Invariants
(GL_n, GL_m)-duality and symmetric plethysm 85

L-function
On the nonvanishing of some L-functions 117
Lattice points
The area within a curve 111
Lobachevsky space
Poincaré series for $SO(n, 1)$ 231
Lost notebook
Hypergeometric series and continued fractions 277

Mean value estimate
Fluctuations in the mean of Euler's phi function 239
Metaplectic group
On the nonvanishing of some L-functions 117
Modular curve
The Manin–Drinfeld theorem and Ramanujan sums 251
Modular forms
On Ramanujan's modular identities 263
Modular functions
Hypergeometric series and continued fractions 277
Modular group
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201
Multiplicative independence of integers
Multiplicative properties of the partition function 297

Non-congruence subgroups
The Manin–Drinfeld theorem and Ramanujan sums 251
Non-uniform lattices
Poincaré series for $SO(n, 1)$ 231

Partition congruences
On Ramanujan's modular identities 263
Partition function
Multiplicative properties of the partition function 297
Plethysm
(GL_n, GL_m)-duality and symmetric plethysm 85
Poincaré series
Poincaré series for $SO(n, 1)$ 231
Poised series
Almost poised hypergeometric series 61
Polynomials
On prime representing polynomials 75
Primes
On prime representing polynomials 75
q-continued fractions
On some generalizations of Ramanujan's continued fraction identities 31
q-series
Hypergeometric series and continued fractions 277

Quaternion orders
Traces of Eichler–Brandt matrices and type numbers of quaternion orders 189
Quaternions
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201

Ramanujan sums
The Manin–Drinfeld theorem and Ramanujan sums 251
Ramanujan τ function
On exponential sums involving the Ramanujan function 157
Ramanujan's modular identities
On Ramanujan's modular identities 263
Ramanujan-type approximations
Explicit Ramanujan-type approximations to pi of high order 53
Reciprocity law
On the proof of the reciprocity law for arithmetic Siegel modular functions 21
(GL_n, GL_m)-duality and symmetric plethysm 85
Recursive approximation to pi
Explicit Ramanujan-type approximations to pi of high order 53
Relative trace formula
On the nonvanishing of some L-functions 117
Rogers–Ramanujan continued fractions
On some generalizations of Ramanujan's continued fraction identities 31
Rogers–Ramanujan identities
On an approximate identity of Ramanujan 313

Selberg–Kloosterman zeta function
Poincaré series for $SO(n, 1)$ 231
Semisimple group
On the set of discrete subgroups of bounded covolume in a semisimple group 45
Siegel ϕ-operator
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201
Siegel space
On the proof of the reciprocity law for arithmetic Siegel modular functions 21

Supercuspidal representation
The characters of supercuspidal representations as weighted orbital integrals 3
Supersingular reduction
On the supersingular reduction of elliptic curves 247
Symmetric plethysm
(GL_n, GL_m)-duality and symmetric plethysm 85
Tensor products
On endomorphisms of degree two 179
Three-term relations
Hypergeometric series and continued fractions 277
Unimodular group
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201
Waldspurger result
On the nonvanishing of some L-functions 117
Weighted orbital integrals
The characters of supercuspidal representations as weighted orbital integrals 3
Whittaker models
On Whittaker models and the vanishing of Fourier coefficients of cusp forms 67

AUTHOR INDEX

Adiga Chandrashekar
see Bhargava S 31

Arthur James
The characters of supercuspidal representations as weighted orbital integrals 3

Baily L Walter Jr
On the proof of the reciprocity law for arithmetic Siegel modular functions 21

Bhargava S
On some generalizations of Ramanujan's continued fraction identities 31

Borel A
On the set of discrete subgroups of bounded covolume in a semisimple group 45

Borwein J M
Explicit Ramanujan-type approximations to pi of high order 53

Borwein P B
see Borwein J M 53

Bressoud M David
Almost poised basic hypergeometric series 61

Gelbert Stephen
On Whittaker models and the vanishing of Fourier coefficients of cusp forms 67

Grosswald Emil
On prime representing polynomials 75

Howe Roger
(GL_n, GL_m)-duality and symmetric plethysm

Huxley M N
The area within a curve 111

Jacquet Herve
On the nonvanishing of some L-functions 117

Jutila M
On exponential sums involving the Ramanujan function 157

Karatsuba A A
Approximation of exponential sums by shorter ones 167

Koecher Max
On endomorphisms of degree two 179

Körner Otto
Traces of Eichler–Brandt matrices and type numbers of quaternion orders 189

Krieg Aloys
The Hecke-algebras related to the unimodular and modular group over the Hurwitz order of integral quaternions 201

Li Jian-Shu
Poincaré series for $SO(n, 1)$ 231

Montgomery L Hugh
Fluctuations in the mean of Euler's ϕ function 239

Murty M Ram
On the supersingular reduction of elliptic curves 247

Murty V Kumar
The Manin–Drinfeld theorem and Ramanujan sums 251

Raghavan S
On Ramanujan's modular identities 263

Ramakrishnan Dinakar
see Murty V Kumar 251

Ramanathan K G
Hypergeometric series and continued fractions 277

Sarnak P
see Li Jian-Shu 231

Schinzel A
Multiplicative properties of the partition function 297

Shapiro-Piatetski
see Li Jian-Shu 231

Somashekara D D
see Bhargava S 31

Soudry David
see Gelbert Stephen 67

Varadarajan V S
The states of the character ring of a compact group 305

Wirsing E
see Schinzel A 297

Zagier D
On an approximate identity of Ramanujan 313